Welcome

Whether you are a Windows 95 user on a desktop, a workstation, or a notebook, at home, work, or school, there is always the risk of your computer being infected by a computer virus. Some computer viruses contain routines which when activated cause all sorts of irreversible damage to your computer system including destroying all of the information on your hard disk.

PC-cillin II is the ideal solution for protecting your Windows 95 system from the harmful effects of a computer virus attack. PC-cillin II is a user-friendly, powerful utility that incorporates advanced anti-virus technology, including powerful features such as 32-bit scanning, online protection, and protected mode real-time scanning. Which simply means, PC-cillin II will find those viruses, before they find you.

{button ,AL(`Features and Benefits;How PC-cillin II Protects You;How PC-cillin II Warns You;Overview of PCcillin 95',0,`',`')} Related Topics

Overview of PC-cillin II

PC-cillin II is an anti-virus utility that provides a complete system of anti-virus features that are specifically designed to protect Windows 95 systems from new virus sources, and increasingly sophisticated types of viruses. PC-cillin II constantly monitors all potential virus sources to trap viruses before they can infect a system.

The emergence of on-line viruses, especially those lurking throughout the Internet, has created an increased threat of infection for any system with a modem or on a network. If not detected, these new virus strains can infect and destroy an entire network in less than an hour. This can be avoided with continuous, proper protection. PC-cillin II maximizes protection for Windows 95 and on-line services without compromising speed or ease of use.

PC-cillin II makes constant protection feasible by intelligent selection of how, what and when to scan files. Specific monitoring is provided for files attached to shared folders, Internet, e-mail, FTP, and other special formats (i.e., compressed files). When you copy, transfer or download files, the risk of getting a virus infection increases because you expose your system to sources that are more likely to be infected with a virus. PC-cillin II is the first smart, self-adjusting anti-virus protection program that pays attention to several possible sources of virus infections. PC-cillin II dynamically adjusts the protection level to the threat level.

PC-cillin II knows what virus sources to watch in Windows 95, when to watch them, and how to properly remove computer viruses, even unknown ones, from your system.

{button ,AL(`Features and Benefits;How PC-cillin II Protects You;How PC-cillin II Warns You',0,`',`')} Related Topics

Features and Benefits

Automatic, On-line Pattern Updates -- Up-to-the-Minute Virus Protection: Keeping your virus pattern file up-to-date is the key to detecting and cleaning many of the newest viruses. Now PC-cillin II does this updating for you automatically by downloading the latest virus pattern files as they become available. PC-cillin II keeps your protection current 24 hours a day!

Clean Wizard -- Your Built-in Virus Expert: Automatic virus removal! Every time PC-cillin II nabs a virus, our one-of-a-kind Clean Wizard instantly springs into action to automatically remove the virus for you step-by-step, without harming your valuable data. It's the virus expert so you don't have to be.

Macro Shield -- The Only True Macro Virus Defense: New Word Macro viruses are being created at a blinding pace. Not only are they extremely difficult to catch before they cause damage, but they can be produced in a matter of minutes by practically anyone. PC-cillin II blocks Word Macro viruses before they have a chance to infect your system. Plus, our patent-pending Macro Shield not only detects and cleans known macro viruses, but will even catch new strains that have yet to be identified.

On-line Protection -- Stops the Cyberspace Virus Invasion: Thousands of viruses are lurking throughout the Internet and on-line services, just waiting to jump through any unprotected modem or Internet connection. But have no fear PC-cillin II stops them cold!

- Scans all Internet and on-line service downloads
- Checks incoming e-mail and attached files
- Scans more types of compressed files than any other anti-virus

Internet Virus Lab -- Your "On-Call" Virus Expert: With PC-cillin II, you not only get the best virus protection in the business, but you also get our one-of-a-kind Internet Virus Lab. Just link up with the Internet Virus Lab using PC-cillin II's built-in ActiveX browser to get up-to-the-minute virus news and information, virus outbreak alerts, and expert virus analysis. Plus, the Internet Virus Lab is staffed 24 hours a day by our highly-trained team of experts, so we're there whenever you need help.

> **We Keep You Informed** -- You no longer have to rely on word-of-mouth or computer magazines to find out about the newest viruses to hit the public. The Internet Virus Lab gives you accurate, up-to-the-minute information on all the latest outbreaks, as well as details on thousands of viruses.
>
> **Emergency Virus Removal Service** -- If you ever find a virus that you just can't get rid of, our experts will take care of it for you. Just click a button and we'll automatically upload any infected files from your system and provide you with a response within three hours. PC-cillin II is the only anti-virus to give you personalized virus protection!

Not Just Total Defense -- Active Defense: PC-cillin II's powerful new Active Defense uses the latest in ActiveX technology to make sure your program is always up-to-date. It automatically loads the latest virus pattern updates, updates your scan engine and downloads the newest virus rules while you work, to keep your protection at the highest level possible around the clock.

{button ,AL(`Advanced Detection Technology;How PC-cillin II Protects You;How PC-cillin II Warns You;NCSA;Virus Monitor;Virus Scanner',0,`',`')} Related Topics

How PC-cillin II Protects You

TouchStone Software and Trend Micro Devices have developed and combined several technologies that compliment each other, to keep your computer virus-free.

These technologies provide increased protection when your risk of infection increases. If a particular virus is able to get past one technology, another one will catch it.

In short, PC-cillin II protects you by:

- Detecting known viruses that may already exist on your computer and removing them.
- Preventing both known and unknown viruses from infecting your computer.
- Monitoring your computer for activity that may indicate an unknown virus.

{button ,AL(`Advanced Detection Technology;Rule-Based Technology;VICE Technology;Cleaning Mutation Viruses',0,`',`')} Related Topics

Advanced Detection Technology

The better anti-virus products use more than one strategy for detecting viruses. Simple pattern scanning, for example, will not catch unknown or mutation viruses. For this reason, PC-cillin II scans for virus instructions, then detects the infected file(s) before they are executed.

{button ,AL(`Cleaning Mutation Viruses;How PC-cillin II Protects You;Rule-Based Technology;VICE Technology',0,`',`')} Related Topics

VICE Technology

The ability to scan new viruses and the removal of their instructional code is accomplished by PC-cillin II's VICE (Virus Instructional Code Emulator) technology.

VICE assists the computer user by immediately analyzing all unknown viruses, polymorphic viruses, and mutation-engine viruses.

After PC-cillin II detects a virus, VICE automatically analyzes the virus and updates PC-cillin II's virus pattern database. VICE simultaneously cleans the infected file by removing the virus code.

{button ,AL(`Advanced Detection Technology;Cleaning Mutation Viruses;How PC-cillin II Protects You;Rule-Based Technology',0,`',`')} Related Topics

Rule-Based Technology

Monitoring for virus activity can be done by installing PC-cillin II resident in memory. PC-cillin II monitors requests that are passed to the interrupt table. Examples of virus activity would be a request to write to a boot sector, opening an executable program for writing, or the virus placing itself resident in memory. Based on certain common actions of viruses, PC-cillin II has a set of rules that can differentiate between virus activity and normal application activity.

Rule-based monitoring makes it possible to stop infection of a file by a virus before it has a chance to damage a file.

{button ,AL(`Advanced Detection Technology;Cleaning Mutation Viruses;How PC-cillin II Protects You;VICE Technology',0,`',`')}
Related Topics

Cleaning Mutation Viruses

PC-cillin II's mutation virus cleaning engine uses advanced code analysis to decide which part of the infected file is actually a virus.

The cleaning engine scans the decrypted code to determine the identity of the particular mutation-engine virus. When a match is found, the cleaning engine cuts the virus from the infected file and restores the normal execution flow of the file.

{button ,AL(`Advanced Detection Technology;How PC-cillin II Protects You;Rule-Based Technology;VICE Technology',0,`',`')}
Related Topics

How PC-cillin II Warns You

If your boot sector is infected

If the boot sector of your hard disk is infected with a virus, PC-cillin II's Boot Wizard appears. However, if the boot sector on a floppy disk you are scanning is infected, PC-cillin II displays a message box indicating the floppy drive, and the name of the file infected.

If your folders are infected

If the folders you are scanning are infected with a virus, PC-cillin II indicates the name of the infected files/folders and displays them in the Clean Page window. To remove the virus(es), click the Clean Wizard button. The Clean Wizard walks you through the steps to remove them.

{button ,AL(`Clean Page;Clean Wizard;How do I remove boot sector viruses?',0,`',`')} Related Topics

How do I register PC-cillin II online?

PC-cillin II includes a feature that allows you to perform an automatic online registration. Registering your product entitles you to technical support as well as information about new products and services.

To register online:

1. Choose Update Pattern Page from the File menu.
2. Or, click the Update Pattern Tab from the main program window. The Update Pattern Page window appears.
3. Click the Register command button.
4. Fill in the details, and click OK.

{button ,AL(`How do I access the BBS or WWW site?;How do I change BBS/Modem settings?;How do I update my Virus Pattern file?;Update Pattern Page',0,`',`')} Related Topics

File Virus Type

This area provides information about the type of File Virus. See also, Types of viruses.

What's This - Memory Resident Type

This area provides information about the part of memory that the Memory Virus resides in. See also, Types of viruses.

The Protection Meter displays the current level of protection based on the current activity of your system. PC-cillin II automatically increases the level of protection when the number of virus threats increase.

The Threat Meter displays the current level of virus threat activity according to your system resource usage. This level increases as the number of threats increase.

The Threat group box lists the system resources that are monitored by PC-cillin II for virus activity.

Floppy Access - monitors the floppy drives for viruses during floppy drive access

Internet/E-Mail Connect - monitors for virus activity on Internet or e-mail connections

Shared Folders - monitors for viruses when other computers connect to your shared folders

Modem Connection - monitors for virus activity during Modem usage

CD-ROM Access - monitors for viruses activity during CD-ROM usage

DOS Prompt Open - monitors for virus activity in DOS boxes

NetWork Neighborhood - monitors for virus activity during Network Neighborhood access

Dial-up Connection - monitors for viruses during Dial-up connections

Direct Cable Connection - monitors for viruses during Direct Cable connections

Displays a lightning bolt next (left) to the activity(ies) currently being used. All actions are monitored for virus activity.

Displays the latest virus pattern file (current version) loaded on your system and recommends the number of days left before you should replace it. Updating allows you to detect and clean the newest viruses codes (signatures) from your system and update the types of files to be scanned.

Shows the version number and date for the virus pattern file loaded on your system as well as recommends the number of days left before you should replace it. Updating allows you to detect and clean the newest viruses codes (signatures) from your system and update the types of files to be scanned.

The Update button provides you with three options to get the latest virus pattern file (e.g., Internet, BBS or floppy disk)

The Virus Watch feature is only available in the Smart Monitor. When your system detects a virus, the Smart Monitor immediately puts itself on a 90-day Virus Watch to increase the system's defense to combat re-infection. The number of days remaining in the current virus watch period is displayed in red.

This meter represents the time remaining in your virus watch. If your Virus Watch period is set at 90 days, and 45 days have passed, the meter will be half full.

Shows the name of the last virus found

Shows the date when the last virus was found

Click this button to open the Virus Watch Setup dialog box

Shows the amount of risk remaining in the Virus Watch period

Recommends when you should scan for viruses

The Scan Update area provides the latest information regarding scans performed on your system, and alerts you to scan all drives when needed (e.g., after updating your virus pattern file).

Shows the number of days since the last full scan

Shows the date of the last full scan

Click this button to perform a full virus scan of your system “on-the-fly”

Click this button to display the relevant online Help topic for this window

Click this button to close the monitor and display the main program window

Click this button to unload (remove the monitor from the taskbar and exit) the program

Click this button to reduce the monitor to an icon on the taskbar

Click this button to switch to the Update Options page

The Protect area allows you to specify which activities PC-cillin II monitors. To select an activity to monitor, click the appropriate check box. Only selected activities are monitored for viruses. For example, to scan only executable and compressed files, select Execute Programs and Compressed files.

Floppy Boot Sector - monitors for viruses in the boot sector of a floppy disk you access

Execute Program - monitors for viruses in executable programs only

File is Opened - monitors for viruses when you open a file

File is Created - monitors for viruses when you create a new file

UUENCODE files - monitors for viruses in UUENCODED files.

Compressed files - monitors for viruses in compressed files

Deny Write - enables the Deny Write feature

DLL Checksum - enables DLL checksum checking

Monitors and scans the file types you specify (keeps track of the file types specified) and displays the name of the file when it is being used

Click this button to configure the program file types (extensions) to monitor

Displays the name of the current file being scanned when it is being used

This meter shows the current status of your CPU activity. When your system activity is high (i.e., several windows are open on your desktop), the monitor level increases. Thus, when your system activity is low, the monitor level decreases.

Type in a program file extension to add to the list. Valid extensions consist of one to three letters (e.g. COM or HH, etc.).

Click this button to close the window saving any changes you have made

Click this button to close the window without saving any changes you have made

Shows the number of infected files, number of files cleaned, current scan action and the name of the last virus found

Shows the total number of files scanned and the path, folder and name of the last file scanned for the current session

Shows the number of files scanned and the time taken to perform the scan for the current session

Shows the name of the file infected by the virus

Shows the name of the virus that infected the file

Shows the current status of the infected file (cleanable, non-cleanable, etc.)

Click this button to start the Clean Wizard. This button is dimmed, if no viruses are detected

Click this button to access the Virus Information page where you can view or print virus descriptions for a particular file or multiple files

Click this button to clean the virus from the selected file

Click this button to delete the selected file

Click this button to rename the selected file to a non-executable extension (e.g., .VIR)

Displays the list of selected program file type extensions that are scanned by the virus scanner

Click this button to add a program file type extension to the list

Click this button to ignore any modifications and accept the default selections

Displays the type of file virus (e.g., cleanable, encrypt, etc.) that applies to the selected virus name

Displays the memory resident type virus (e.g., OS, MCB, etc.) that applies to the selected virus name

This drop-down list allows you to specify when a scheduled scanning session will occur (e.g., Everyday, Once a Week, Once a Month or Never).

This area allows you to designate the time of day a scheduled scan will occur.

If the frequency of a scheduled scan is set at once a week, this drop-down list allows you to specify which day of the week the scan will occur.

If the frequency of a scheduled scan is set at once a month, this drop-down list allows you to specify which day of the month the scan will occur.

Click this button to choose the drive(s) you want to scan

Select this option to scan all files (recommended).

Select this option to scan only selected files.

Select this option to check the boot area for viruses during scan operations (recommended).

Select this option to scan compressed files (e.g., PKZIP, PKLITE, LZEXE, LHA, Microsoft Compressed, and ARJ files).

Select this option to create a scan report upon completion of a scanning session.

Shows the location (pathname, folder) and filename of the scan report.

Select this option to view a scan report instantly upon completion of a scanning session.

Choose the application you would like to view the scan report in. For example, you could select WORDPAD or MS WORD.

Click this button to open the Browser and make a selection

System Startup options allow you to specify if PC-cillin II will scan your system's memory and boot area when you boot your system

Select this option to scan memory for viruses every time your system starts up (recommended)

Startup Options allow you to specify if PC-cillin II will dock on the taskbar or automatically load PCSCAN into your AUTOEXEC.BAT file every time you start your computer

Select this option to scan for viruses every time your computer is started (recommended)

Select this option to dock the program into the Windows 95 Taskbar every time you start your computer

Select the Smart Monitor or Custom Monitor option to enable that monitor

Selects the Smart Monitor and displays it every time you access the program

Click this button to configure Smart Monitor options

Selects the Custom Monitor and displays it every time you access the program

Click this button to configure Custom Monitor options

Select this option to monitor all files accessed for viruses

This feature protects executable files in a selected folder/sub-folder from being modified in any way

Click this button to select the folder/sub-folder you want to protect

Allows you to modify the IP Address and Pattern File Directory settings for Internet access

Allows you to configure/modify Modem settings

Allows you to configure/modify BBS settings

Select the drive(s)/folder(s) you want to scan in the directory tree. Click on the + or - to expand or collapse folders. Selected drive(s)/folder(s) will have a check mark placed in the box

Click this button to start scanning the selected drive(s)/folder(s)

Click this button to switch to the Scan Options page

Click this button to update the directory tree with the most recent information

Select this option to perform a quick scan only (scan boot area and root directory of C drive)

Select this option to scan ‘‘all the local drives’’ on your computer

Select this option to scan ‘‘all the network drives’’ attached to your system

Click the Internet, BBS or Floppy button to update your virus pattern file with the latest data

Click this button to register PC-cillin II online

This bar graph indicator shows how far along the update pattern routine has progressed in terms of a percentage of completion

Click this button to switch to the Update Options page

Click the Stop button to abort the pattern file update

This drop-down list allows you to select the virus types you want to view (e.g., Common Viruses, File Viruses, Macro Viruses, boot viruses or All Viruses)

Displays an alphabetical listing of virus names

A description of the selected virus is shown here, if one is available

Click this button to print out the virus information

Click this Tab to switch to the Scan Page

Click this Tab to switch to the Clean Page

Click this Tab to switch to the Update Pattern Page

Click this Tab to switch to the Virus Information Page

This bar graph indicator shows you how far along the virus cleaning routine has progressed in terms of a percentage of completion

Click this button to return to the previous window

Click this button to continue to the next window

Select this option to scan your local drives now

Select this option to scan your local drives later

This function is dimmed.

Click this button to view a log of cleaned files

Click this button to complete the current procedure

Displays the default e-mail message that you can modify when PC-cillin II detects a virus

Click this button to send the e-mail message

Click this button to print the e-mail message

This drop-down list allows you to select a floppy drive to scan

Click this button to scan the next floppy

Displays the filename(s) infected by a virus

Click this button to print instructions on how to remove the virus

Click this Tab to switch to the Scan Options Page

Click this Tab to switch to the Update Options Page

Click this Tab to switch to the Preschedule Options Page

Click this Tab to switch to the Startup Options Page

The protect and threat meters show the current level of anti-virus security according to the "current activity" on your system. The protect meter indicates how hard PC-cillin II is working to keep your system secure. The level increases when the number of threats increase. The threat meter indicates how many threats are currently active (i.e., Modem Connection, Floppy Access, etc.). The level increases when the threats increase.

Virus Monitor

PC-cillin II's Virus Monitor consists of two components, a Smart Monitor and a Custom Monitor. Both these monitors constantly analyze your system for all types of virus activity. A warning is given when any viruses are detected.

Smart Monitor - PC-cillin II's Smart Monitor automatically adjusts protection levels, detects and eliminates unknown viruses, scans Internet transfers and E-mail attached files, and keeps your virus protection up-to-date with easy, one-button virus pattern updates.

Custom Monitor - The Custom Monitor provides you with the same type of protection as the Smart Monitor, but it allows you to specify which activities you want to monitor. You can also configure the program file type extensions you want to protect against virus infection.

Unless you are an experienced computer user that is familiar with computer viruses, we recommend using the Smart Monitor.

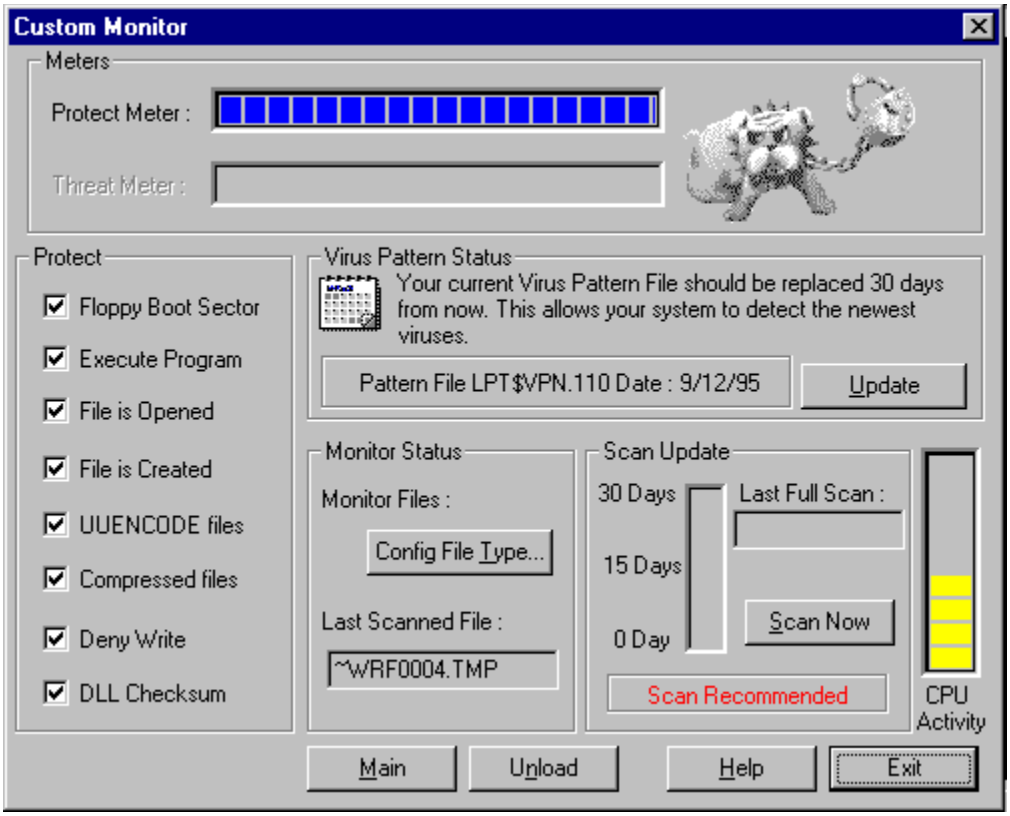
{button ,AL(`Custom Monitor;Smart Monitor',0,`',`')} Related Topics

Custom Monitor

The Custom Monitor was designed with the power-user in mind. The Custom Monitor provides you with the same type of protection as the Smart Monitor, but it allows you to specify which activities you want to monitor. You can also configure the program file type extensions you want to protect against virus infection. The Custom Monitor performs virus scans in the background without affecting normal operations. Files you select in the Protect area are scanned for viruses BEFORE they are executed, copied, saved or created. When a virus is detected in a specified file type, PC-cillin II stops the virus before it can do any harm. The Custom Monitor continually monitors your system and performs virus scans in the background without affecting normal operations until you unload the program.

{button ,AL(`Custom Monitor Window;Manual Scans;Reading the Protect and Threat Meters',0,`',`')} Related Topics

Custom Monitor Window - Click on the area you would like more information on.

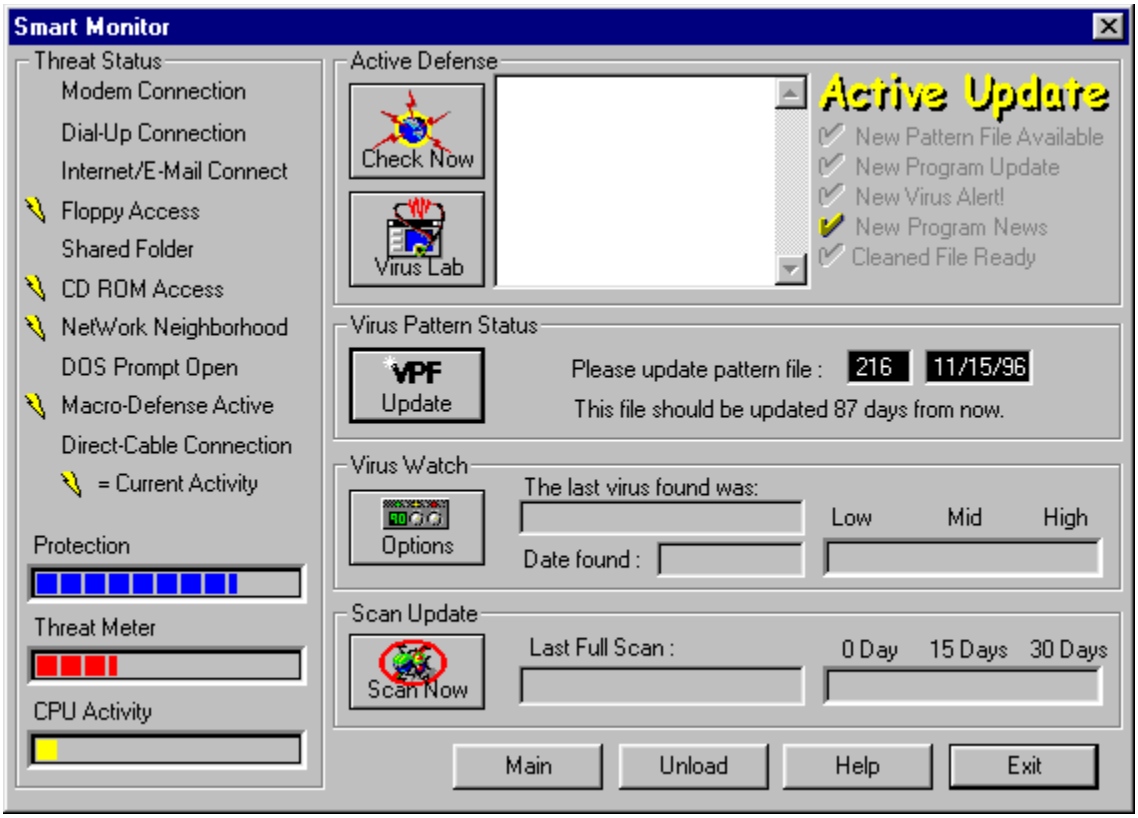


{button ,AL(`Custom Monitor;Virus Monitor',0,`',`')} Related Topics

Smart Monitor

PC-cillin II's "Smart Monitor" automatically adjusts protection levels, detects and eliminates unknown viruses, scans Internet transfers and E-mail attached files, and keeps your virus protection up-to-date with easy, one-button virus pattern updates. PC-cillin II is equipped with the ability to automatically adjust the level of protection based on the threat and independently execute virus scans as needed, so you do not have to think about it. The Smart Monitor continually monitors your system and performs virus scans in the background without affecting normal operations until you unload the program.

Smart Monitor Window - Click on the area you would like more information on.



{button ,AL(`Smart Monitor;Virus Monitor',0,`',`')} Related Topics

Automatic Scans

PC-cillin II is its own built-in expert; it determines when to scan for viruses and automatically monitors your computer. PC-cillin II automatically adjusts the level of protection based on the current activity (threat), and executes virus scans as needed. These scans trap and eliminate known viruses before they can infect your system. PC-cillin II's Smart Monitor performs automatic scans each and every time you copy a file from a floppy disk or download files from an online service or network/Internet connection.

{button ,AL(`Custom Monitor;Custom Monitor Window;Manual Scans;Scheduled Scans;Smart Monitor;Smart Monitor Window',0,`',`')} Related Topics

Manual Scans

You can perform manual scans by clicking the Scan Now command button in the Smart Monitor or Custom Monitor window, or by dragging and dropping a folder on the Scan Page window. Manual scans also catch changes to your system files, which may indicate an unknown virus. Use manual scans to verify that your computer and floppy disks are free of viruses.

{button ,AL(`Custom Monitor Window;Determining When To Scan;How do I scan on-the-fly?;Scan Page;Smart Monitor Window',0,`',`')} Related Topics

Reading the Protect and Threat Meters

The protect and threat meters show the current level of anti-virus security according to the ‘‘current activity’’ on your system. For example, when you are loading a new software application, or simply copying a folder off the network, PC-cillin II automatically monitors those activities and calculates which preventative actions are required.

{button ,AL(`Custom Monitor Window;Smart Monitor Window;Virus Threats',0,`',`')} Related Topics

Determining When To Scan

Computer viruses can exist in two forms—either active in your computer's memory or lying dormant in floppy or hard disk files and boot record. It is crucial to scan these environments for viruses to prevent infection of your system.

When you insert a new diskette

Every time you insert a new diskette into your floppy drive(s), you should scan it before executing, installing or copying its files. If you share diskettes with co-workers or friends, or the diskettes have been in another PC, we recommend scanning them for viruses before any harm can come to pass.

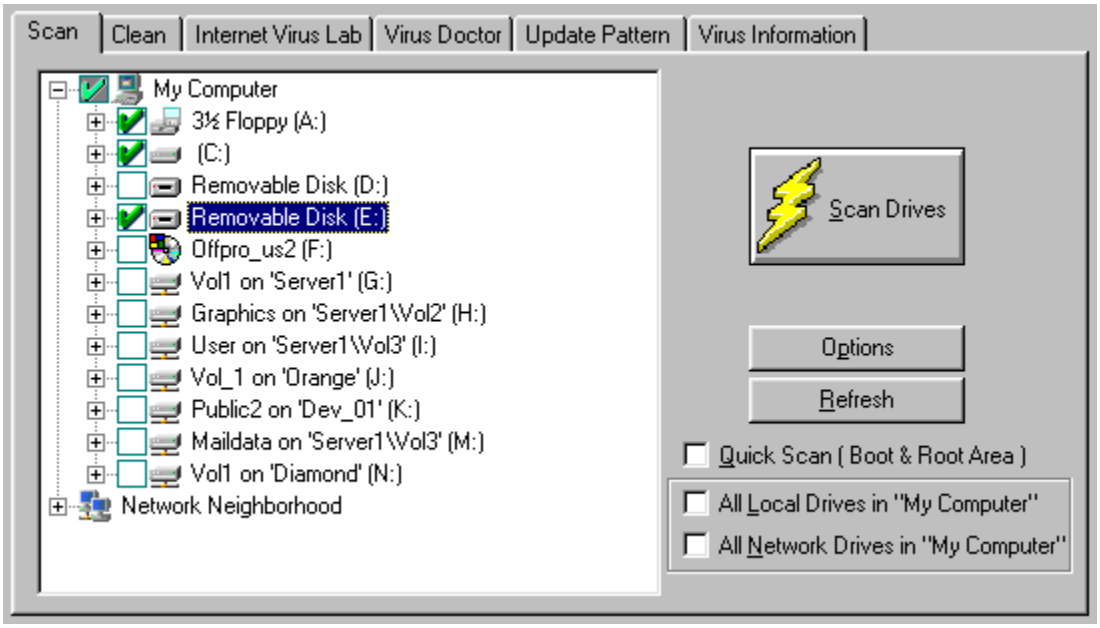
When you install or download new files

Every time you install new software on your hard drive, or download executable files from a network server, BBS, or online service (i.e., CompuServe), you should scan the folders/sub-folders in which the files were placed before the files are executed.

When PC-cillin II is loaded and monitoring your system, every time you download a new file, PC-cillin II automatically scans that file so you don't have to think about it. If a virus is detected, the Clean Page window appears displaying the name of the file(s) infected. You can remove the virus, using the Clean Wizard or Clean, Delete, and Rename command buttons.

{button ,AL(`Can I keep my computer virus-free?;Types of viruses;Virus Threats',0,`',`')} Related Topics

Scan Page - Click on the area you would like more information on.



{button ,AL(`How do I pause a scanning session?;How do I refresh the directory tree?;How do I scan a drive?;How do I scan a folder?;How do I scan for viruses?;How do I scan local drives?;How do I scan network drives?;How do I scan on-the-fly?;How do I stop a scanning session?',0,`',`')} Related Topics

How do I scan for viruses?

You can start a virus detection and removal routine by clicking on the Scan Drives command button in the Scan Page window. Once you click the Scan Drives command button to begin the detection (and removal) process, the Scanner Report window appears displaying a bar graph indicator that shows you how far along the virus detection routine has progressed in terms of a percentage of completion. You see the pathname, folder(s), and filenames being scanned.

To start a virus scan:

1. Launch the PC-cillin II application.
2. From the Scan Page window, select one or more of the following options: Scan C Root Directory, All Local Drives in My Computer or All Network Drives in My Computer.
3. Or select the drive/folder you want to scan.
4. Click the Scan Drives command button.

{button ,AL(`How do I scan a drive?;How do I scan a folder?;How do I scan local drives?;How do I scan network drives?;How do I scan on-the-fly?;Scan Page',0,`',`')} Related Topics

How do I scan a folder?

To scan a folder:

1. Drag-and-drop a folder/sub-folder onto the Scan Page window.
2. Or, choose Scan Page from the File menu.
3. To select every folder/sub-folder on a particular drive, double-click the drive(s) box you want to scan.
4. If necessary, you can deselect a folder within a folder.
5. Expand the selected drive list by clicking the + sign (selected folders will have a check mark placed next to them).
6. Click the folder(s) you do not want to scan (clicking the folder(s) removes the check mark).

{button ,AL(`How do I pause a scanning session?;How do I stop a scanning session?;Scan Page;Virus Scanner',0,`',`')} Related Topics

How do I scan a drive?

To scan a drive:

1. Choose Scan Page from the File menu.
2. Or, select the Scan Tab from PC-cillin II's main program window. The Scan Page window appears.
3. Select one or more of the following options: Quick Scan (Boot & Root Area), All Local Drives in "My Computer" or All Network Drives in "My Computer."
4. Or, click the drive box(es) you want to scan.
5. To begin scanning, click the Scan Drives command button.

{button ,AL(`How do I pause a scanning session?;How do I stop a scanning session?;Scan Page;Virus Scanner',0,`',`')} Related Topics

How do I scan on-the-fly?

To scan on-the-fly:

1. Choose Programs, Windows Explorer from the Start menu.
2. Drag-and-drop a folder onto any PC-cillin II main program window (i.e., Scan Page, Clean Page, etc.).
3. Or, right-click the folder you want to scan. A pop-up menu appears. From the pop-up menu, choose PC-cillin II. This action scans every file within the selected folder. You can select multiple folders.

   The Scanner Report window appears informing you of the progression of the scan.

{button ,AL(`How do I pause a scanning session?;How do I stop a scanning session?;Scan Page;Virus Scanner',0,`',`')} Related Topics

How do I pause a scanning session?

PC-cillin II gives you the ability to pause an active scanning session.

To pause scanning:

1. From the Scanner Report window, click the Pause button. This action causes the Pause button to switch to the Continue button and temporarily stops the scanning process.
2. To reactivate the scanning process, click the Continue button.

   Note: Each time you click the button, it toggles back and forth between Pause and Continue.

{button ,AL(`How do I stop a scanning session?;Scan Page',0,`',`')} Related Topics

How do I stop a scanning session?

PC-cillin II gives you the ability to stop an active scanning session.

To stop scanning:

1. From the Scanner Report window, click the Stop button. This action displays the **Do you want to stop the scan process?** message box.
2. To continue scanning, click the No button.
3. To abort the scanning session, click the Yes button.

{button ,AL(`How do I pause a scanning session?;Scan Page',0,`',`')} Related Topics

How do I refresh the directory tree?

Refreshing the directory tree allows you to view the latest data on your system. The Refresh button clears the directory tree and redisplays the list showing any recent activity. An example when you may need to refresh a directory is: if you remove or add folder(s), and/or download folders/files from an online service or network connection.

To refresh the directory tree:

1. From the Scan Page window, click the Refresh button.

   PC-cillin II clears the directory tree and redisplays it on your computer showing any updated activity.

{button ,AL(`Scan Page',0,`',`')} Related Topics

How do I scan local drives?

To scan all local drives:

1. Choose Scan Page from the File menu.
2. Or, select the Scan Tab in PC-cillin II`s main program window. The Scan Page window appears.
3. Select the All Local Drives in My Computer check box.
4. To begin scanning, click the Scan Drives command button.

{button ,AL(`Scan Page',0,`',`')} Related Topics

How do I scan network drives?

To scan all network drives:

1. Choose Scan Page from the File Menu
2. Or, select the Scan Tab from PC-cillin II`s main program window. The Scan Page window appears.
3. Select the All Network Drives in My Computer check box.
4. To begin scanning, click the Scan Drives command button

{button ,AL(`Scan Page',0,`',`')} Related Topics

Virus Cleaner

PC-cillin II's powerful Virus Cleaner removes viruses from infected files.

When PC-cillin II detects a virus, the virus name and the name of the infected file(s) appears in the Infected File Name text box in the Clean Page window.

PC-cillin II offers three ways to deal with viruses: deleting the infected file(s), renaming the infected file(s), or cleaning the infected file(s). As you perform an action on a virus, that virus is removed from the list. When you have deleted, renamed and cleaned all the detected viruses, the list box will be empty.

When you know or suspect that a virus infection has occurred, a special Clean Wizard walks you through the removal process step-by-step to avoid re-infection, and ensure that the virus is removed properly -- without harming the system's files. If a virus is resident in memory, the most secure way to clean your system is to turn off your computer and start from a clean start-up diskette (i.e., emergency rescue disk).

{button ,AL(`Clean Page;Clean Wizard;Cleaning virus infected files;How do I clean an infected file?;How do I delete an infected file?;How do I remove a virus?;How do I rename an infected file?',0,`',`')} Related Topics

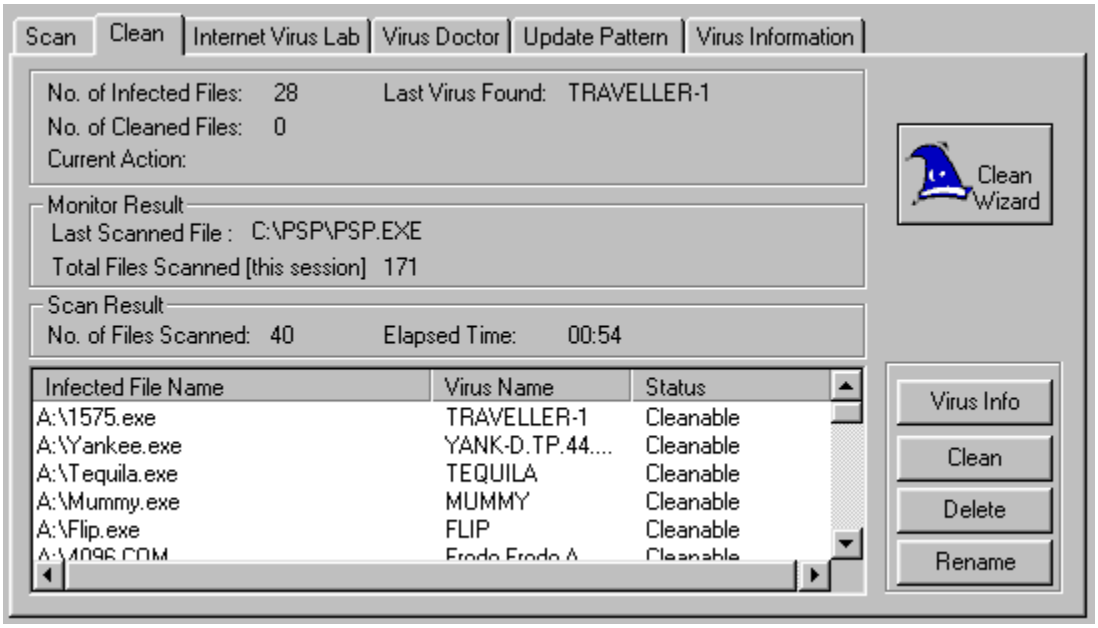
Cleaning virus infected files

PC-cillin II includes a cleaning engine that attempts to remove the virus from an infected file, leaving the original file undamaged. However, some viruses damage files during the infection process. Therefore, you cannot safely clean some files.

When you select OK, PC-cillin II will begin cleaning the file(s). If the cleaning was successful, the file(s) will be removed from the infected files list box. However, if the cleaning was not successful, you will receive a warning prompt. At this point, you must delete or rename the infected file because it cannot be cleaned.

{button ,AL(`Clean Page;Clean Wizard;How do I clean an infected file?;How do I remove a virus?',0,`',`')} Related Topics

Clean Page - Click on the area you would like more information on.



{button ,AL(`Clean Wizard;Cleaning virus infected files;How do I clean an infected file?;How do I delete an infected file?;How do I remove a virus?;How do I rename an infected file?',0,`',`')} Related Topics

How do I remove a virus?

PC-cillin II offers you three methods in which to remove a virus: delete the infected file(s), rename the infected file(s), or clean the infected file(s). As you perform an action on a virus, that virus is removed from the list. When you have deleted, renamed, and cleaned all the detected viruses, the list box will be empty.

{button ,AL(`Clean Page;Clean Wizard;Cleaning virus infected files;How do I clean an infected file?;How do I delete an infected file?;How do I remove boot sector viruses?;How do I rename an infected file?',0,`',`')} Related Topics

How do I clean an infected file?

Cleaning a virus-infected file ‘‘removes’’ the virus from the original file, leaving the original file undamaged. PC-cillin II includes a cleaning engine that attempts to remove the virus from the infected file leaving the original file intact (undamaged). However, some viruses damage files during the infection process; therefore, some files cannot be safely cleaned.

To clean an infected file:

1. From the Clean Page window, under the Infected File Name list box, select the file(s) you want to clean.
2. Click the Clean command button. The **Clean 1 File(s)?** message box appears.
3. To abort cleaning the infected file(s), click the CANCEL command button. To clean the infected file(s), click the OK command button.
4. If the cleaning operation is successful, the **1 file(s) have been cleaned** message box appears.
5. To continue, click the OK command button. PC-cillin II will begin cleaning the file(s). The file(s) are cleaned and removed from the infected files list box.
6. If the cleaning was successful, the file(s) will be removed from the infected files list box. However, if the cleaning was not successful, you will receive a warning prompt. At this point, you must delete or rename the infected file because the file cannot be cleaned.

WARNING!: Even if PC-cillin II "successfully" cleans an infected file, you should test the file before using it. The virus may have damaged the file in ways that PC-cillin II could not detect.

{button ,AL(`Clean Page;Clean Wizard;Cleaning virus infected files;How do I remove a virus?',0,`',`')} Related Topics

How do I delete an infected file?

Deleting a virus infected file results in the virus -- and the infected file -- being deleted. This is the safest way to kill a virus, but it also destroys the infected file. However, if you have backups of the original file (or you can re-install the file), then using Delete is the best measure. If you can restore the infected file from a backup or installation disk, make sure that those disks are not infected, too. Otherwise, you'll just be loading the virus back onto your computer.

To delete an infected file:

1. From the Clean Page window, under the Infected File Name list box, select the file(s) you want to delete.
2. Click the Delete command button. The Delete 1 file(s)? message box appears.
3. To abort deleting the infected file(s), click the CANCEL command button. To delete the infected file(s), click the OK command button. If the deletion operation is successful, the 1 file(s) have been deleted message box appears.
4. To continue, click the OK command button. The file(s) are removed from the source (i.e., floppy disk, etc.) and the infected files list box.
5. To continue, click the OK command button.

   Control returns to the Clean Page window.

{button ,AL(`Clean Page;How do I remove a virus?',0,`',`')} Related Topics

How do I rename an infected file?

Renaming an infected file is only a temporary measure—it does not clean the virus; it simply changes the filename so that the file cannot execute. If you select this action, the file will be renamed with a .VIR extension (i.e., test.exe becomes test.vir). However, if the same filename already exists with the .VIR extension, the filename is renamed with a .VR2 extension (i.e., test.com becomes test.vr2).

PC-cillin II does not limit you on the total number of files that can be renamed, but you are limited to renaming the same filename up to 10 times.

To rename an infected file:

1. From the Clean Page window, under the Infected File Name list box, select the file you want to rename.
2. Click the Rename command button. The Rename 1 File(s) message box appears. To abort renaming the infected file, click the CANCEL command button. To rename the infected file, click the OK command button.
3. To rename additional files, repeats steps 1 and 2 above.
4. If the rename operation is successful, a message box appears telling you what the filename is. To continue, click the OK command button. The renamed file is displayed in the infected files list box.
5. If the rename operation is not successful, a message box appears telling you there is a Rename error! To continue, click the OK command button. The 0 file(s) have been renamed to xxxxxx.vir message box appears.
6. To continue, click the OK command button. Control returns to the Clean Page window.

{button ,AL(`Clean Page;How do I remove a virus?',0,`',`')} Related Topics

Updating PC-cillin II regularly

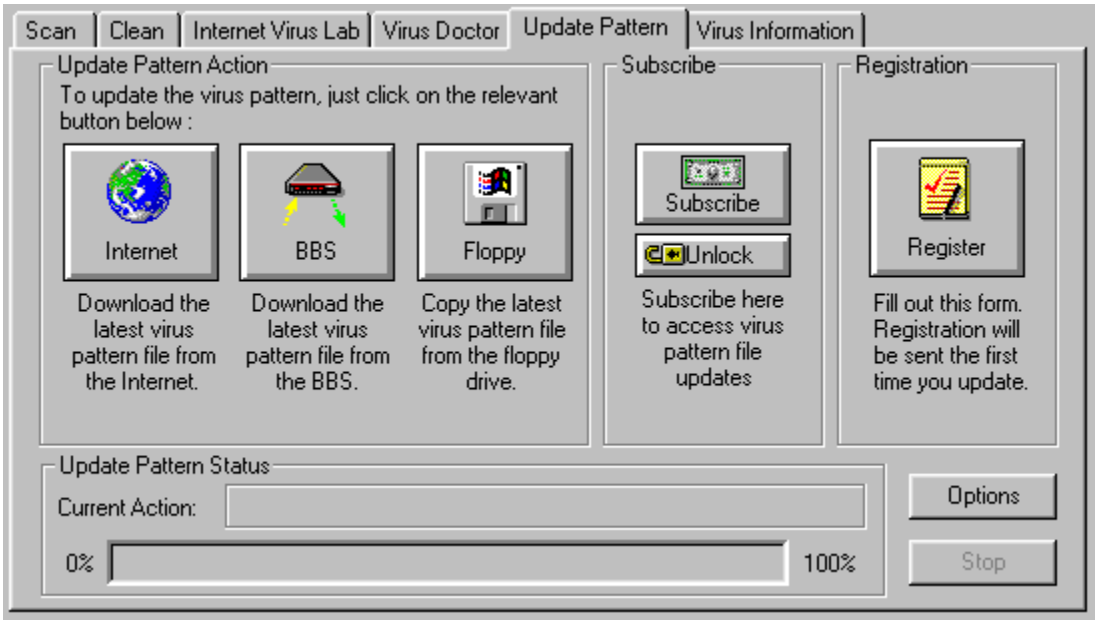
PC-cillin II uses a virus pattern file to detect known computer viruses. By regularly updating your pattern file, you enable PC-cillin II to detect the newest viruses.

To prevent newly discovered viruses from invading your computer, you should periodically update your pattern files. PC-cillin II uses the information in these virus pattern files to detect and eliminate viruses found during scans. When new viruses are found, their virus definitions are added to the virus pattern files. To ensure that you have maximum security against acquiring virus infections, we recommend updating your virus pattern file on a monthly basis.

You can find current information regarding your virus pattern file in the Smart Monitor or Custom Monitor window.

{button ,AL(`How do I update my Virus Pattern file?;Update Pattern Options;Update Pattern Page',0,`',`')} Related Topics

Update Pattern Page - Click on the area you would like more information on.



{button ,AL(`How do I update my Virus Pattern file?;Update Options Page;Update Pattern Options;Updating PC-cillin II regularly',0,``,`')} Related Topics

How do I update my virus pattern file?

PC-cillin II offers you three ways to update your virus pattern files. As a registered owner, you have around-the-clock access to PC-cillin II's BBS, or World Wide Web server on the Internet to download the latest virus pattern file. Choose the one most convenient for you.

- **Internet:** Downloads the latest virus pattern file from the Internet. To use our World Wide Web site, be sure you have an account set up with a service provider before selecting this option.

  You must subscribe to PC-cillin II's services before you can download virus pattern files via the Internet. For more information, see How do I subscribe to virus pattern file updates.

- **BBS:** Downloads the latest virus pattern file from the BBS. You can download virus pattern files for free.

- **Floppy:** Copies the latest virus pattern file from a floppy diskette.

To update your virus pattern file:

1. Choose Update Pattern Page from the File menu.
2. Or, select the Update Pattern Tab from PC-cillin II's main program window.
3. Select the update method you want--click either the Internet, BBS or Floppy button.

   Note: If you select the Internet or BBS options, it automatically connects to PC-cillin II's World Wide Web service forum or BBS and quickly downloads the latest virus pattern update.

   The Update Pattern Status group box displays the status of the current update action, and the bar graph indicator shows how far along the update pattern routine has progressed in terms of a percentage of completion.

Service Providers That Work

PC-cillin II should work with any browser that is capable of supporting the Windows 95 32-bit TCP/IP protocol stacks for the single button download.

For the Internet/Email Monitor option, PC-cillin II works with the following browsers:

In-Box - Microsoft Exchange for Windows 95
Lotus cc:Mail
cc:Mobil
Netscape
Internet Explorer for Windows 95
WS_FTP32
Forte Agent
Telnet
FTP
NCSA Mosaic
Spry Mosaic
Air Mosaic
NetCruiser

{button ,AL(`How do I access the BBS or WWW site?;How do I change BBS/Modem settings?;Update Options Page;Update Pattern Options;Update Pattern Page;Updating PC-cillin II regularly',0,`',`')} Related Topics

How do I subscribe to virus pattern file updates?

For optimum protection against viruses, you must continue to update your virus pattern file after your initial ninety-day free period expires (see **Registering**). We make it easy to maintain your virus pattern files through a one-time subscription process.

You subscribe for 365 days at a time, and that period begins the day you submit the subscription. If you subscribe during your ninety-day free period, the 365 days are added to the remainder of your free period. In other words, if you subscribe on day #60 of your free period, you would have 395 (365 + 30) days of access to the Virus Lab and pattern files.

If your ninety-day free period expires and you try to access the Virus Lab or BBS, a message box appears stating that your free period has expired and that you have to subscribe to PC-cillin II's service. You may do so at this time.

In no way does any of the subscription process affect your ability to reach TouchStone's Technical Support staff as outlined in the Technical Support Policy.

What Do You Get?

When you subscribe to PC-cillin II's services, you receive access to the Internet Virus Lab Check-Up Center, an on-line Virus Newswatch Newsletter, the Internet Virus Doctor, the Internet Instant Support area, and virus pattern file downloads via the Internet (as opposed to TouchStone's BBS, which is free of charge).

For more information on each of these services, see Internet Virus Lab and Internet Virus Doctor.

Subscribing to Virus Pattern File Updates

You can subscribe to PC-cillin II's services at any time using the **Subscribe** button in the Update Pattern window. This will give you unlimited access to the Internet Virus Lab and virus pattern updates for a period of 365 days from the day you subscribe.

When you click on the **Subscribe** button, you are given the choice of subscribing over the Internet or by fax/mail.

Subscribing Over the Internet
Subscribing by Fax/Mail
Unlocking a Subscription

Subscribing Over the Internet

If you click on the **Subscribe** button under the Internet section, PC-cillin II opens your default browser (e.g. Netscape), as defined in your Windows 95 registry, and links to a fulfillment house called CyberSource via their web site, WWW.SOFTWARE.NET. PC-cillin opens the browser to provide a secure means of ordering the subscription and providing a credit card number -- something ActiveX is not yet able to do. This way, your credit card number is perfectly safe -- no one can get to it.

You will be linked to an on-line order form. Fill it out and make sure to include your credit card type (VISA, Master Card, or American Express), card number, and the card's expiration date.

NOTE: You can download new virus pattern updates from the BBS for free.

Subscribing by Fax/Mail

If you click on the **Subscribe** button under the Fax/Mail section, a product registration window appears.

At the top of the screen, several read-only fields display pertinent information about your specific version of PC-cillin II. They include the installation number (an identification number used for obtaining service), serial number, product name (PC-cillin II), program version, and service expiration date.

In the proper fields, fill in the following: first and last name; e-mail address; street address including city, state/province, zip code, country; home, work, and fax phone numbers; company name; and date of purchase in month-day-year format.

Note the asterisks (*) next to the fields that are mandatory.

In the lower right, select a credit card type from the pull down list. Your options are VISA, Master Card, and American Express. Also, include the credit card number and the card's expiration date.

When you have filled in all the proper fields, click on the **Print** button. A standard Windows print dialogue will appear, letting you print the form. From there, you can fax or mail the form.

NOTE: You can download new virus pattern updates from the BBS for free.

Unlocking a Subscription

When you subscribe to PC-cillin II's services, you are given a special unlock code based on your installation and serial numbers.

To unlock your subscription, click on the **Unlock** button under the **Subscribe** button on the Update Pattern tab. A confirmation dialog appears.

Enter the code, then click on the **OK** button. After this, you should have complete access to the Internet Virus Lab and virus pattern updates.

You will also use this procedure to re-activate a lapsed subscription.

Scheduling Virus Pattern File Updates

You can schedule updates to your virus pattern file that can be downloaded automatically on specific dates and times. If you are using the computer when the scheduled update begins, it runs in the background so that you do not have to stop working.

To Schedule an Update

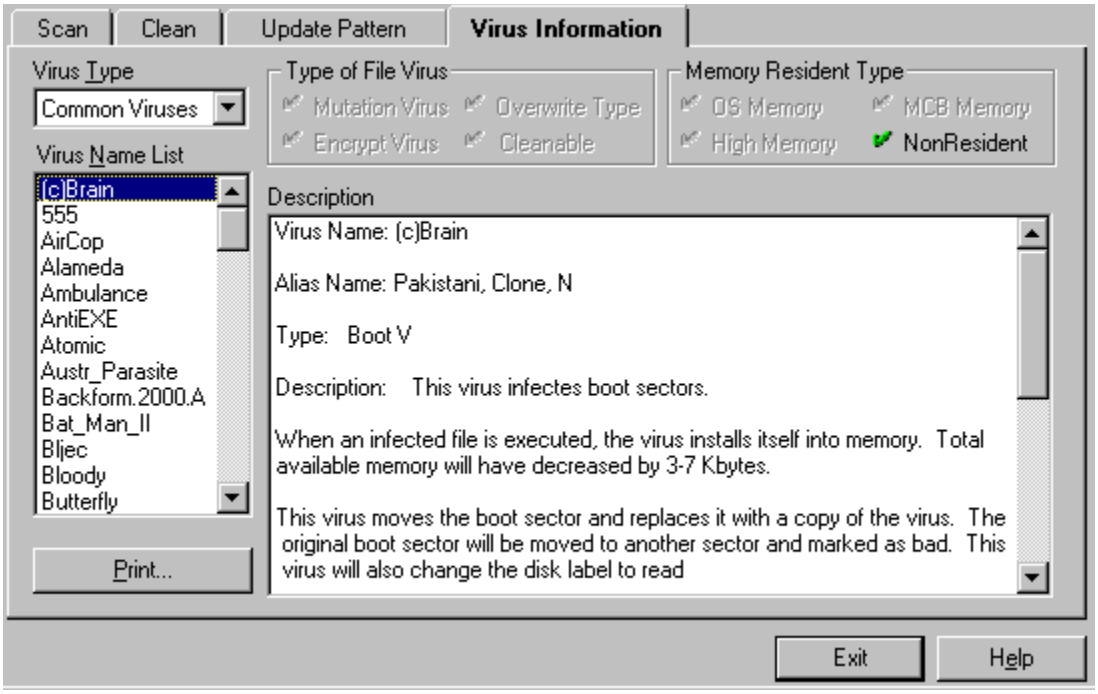
1. Choose Preschedule Options from the Options menu. Or, from the Scan tab, click the **Options** button to display the Options dialog box, then select the Preschedule tab. The Preschedule tab appears.
2. On the right side of the screen, under Preschedule Pattern Update, select how often you want the scan to occur in the Frequency drop-down list: Every Day, Once A Week, or Once A Month.
3. In the hour/minute text boxes, enter the time or click the arrow button(s) to select the time you want the update to occur.
4. To update on a weekly basis, select which day of the week you want the update to occur. Or, to update on a monthly basis, in the Day of Month field, enter or select which day of the week you want the update to occur.
5. Choose method by which updates will be obtained by selecting either the Update Using Internet or Update Using BBS radio button.
6. When you are finished scheduling the update, click the **OK** button.

Virus Information

PC-cillin II includes a list of all the viruses it recognizes (common, boot, or file). Each virus is listed by its more common name, with known aliases shown under the name. The virus list also specifies the type of virus, the size of the virus code, the type of damage the virus causes, and the infection method of the virus.

{button ,AL(`How do I print virus information?;How do I view virus information?;Types of viruses;Virus Information Page;What is a virus?',0,`',`')} Related Topics

Virus Information Page - Click on the area you would like more information on.



{button ,AL(`How do I print virus information?;How do I view virus information?;Types of viruses;Virus Information;What is a virus?',0,`',`')} Related Topics

How do I view virus information?

PC-cillin II includes a list of all the viruses it recognizes (common, boot, or file). Each virus is listed by its more common name, with known aliases shown under the name. The virus list also specifies the type of virus, the size of the virus code, the type of damage the virus causes, and the infection method of the virus.

To view information about a virus:

1. Choose Virus Information from the File menu.
2. Or, choose the Virus Information Tab from PC-cillin II's main program window. The Virus Information window appears.
3. From the Virus Type drop-down list, select the virus type you want information about.
4. Scroll through the Virus Name List and select the virus name you want information about. Information about the virus you selected appears in the Type of File Virus, Memory Resident Type and Description areas.

How do I print virus information?

To print information about a virus:

1. Choose Virus Information from the File menu.
2. Or, choose the Virus Information tab from PC-cillin II's main program window. The Virus Information page appears.
3. Scroll through the Virus Name list box and select the virus name you want information about.
4. To print the virus information, click the Print button. The Print dialog box appears.
5. In the Name field, select or type the printer you want.
6. Click the OK button.

   The virus name you selected prints on the specified printer.

To print a detectable virus list:

1. Choose Detectable List from the Help menu. The List of Detectable Viruses appears.
2. To print the detectable viruses list, click the Print button. The Print dialog box appears.
3. Select the printer you want to print the list on.
4. Click the OK button.

   The detectable viruses list prints on the specified printer.

{button ,AL(`Types of viruses;Virus Information;Virus Information Page;What is a virus?',0,`',`')} Related Topics

How do I remove boot sector viruses?

Using PC-cillin II, boot sector viruses can be destroyed before they have an opportunity to infect your system. However, some boot sector viruses cannot be cleaned from within Windows 95.

If the boot sector on a floppy disk is infected, PC-cillin II displays a message box indicating the floppy drive, and the name of the file infected. However, if the boot sector on your hard drive becomes infected, PC-cillin II's Boot Wizard steps you through the process of removing it.

To remove a boot sector virus (from a floppy disk)

1. When a boot sector virus is detected, a message box appears asking you if you want to remove the virus. The name of the virus is shown in the message box.
2. To abort the removal of the virus, click the No button. To remove the virus, click the Yes button. The **Boot virus removal successful**! message box appears informing you that the virus was successfully removed.
3. To continue, click the OK button. The File scan completed message box appears.
4. To complete the removal procedure, click the OK button. Control returns to the Scan Page window.

{button ,AL(`How do I create a Clean Boot Disk?;How do I create a Rescue Disk?;Boot Wizard',0,`',`')} Related Topics

Boot Wizard

PC-cillin II's Boot Wizard appears when a boot sector virus is detected while you are starting up Windows 95. If the boot sector on your hard drive becomes infected, PC-cillin II's Boot Wizard steps you through the process of removing it.

To remove a boot sector virus (using the Boot Wizard):

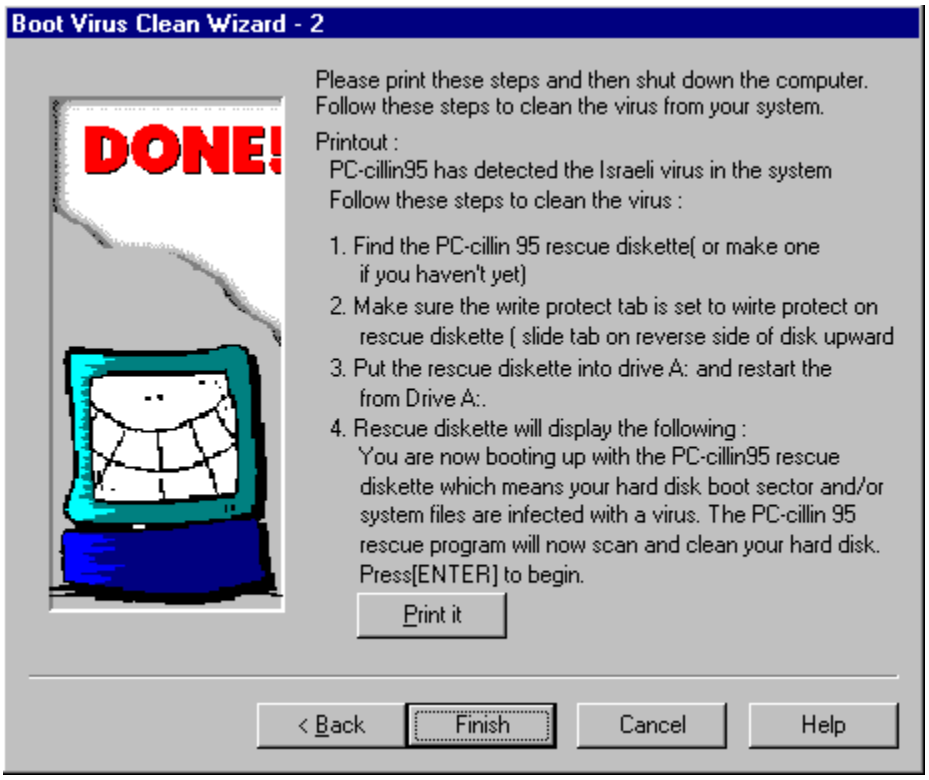
1. When a boot sector virus is detected on your hard disk during the startup phase of Windows 95, the Boot Virus Clean Wizard - 1 window appears.
2. To remove the virus, click the Next button. The Boot Virus Clean Wizard - 2 window appears.
3. Follow the instructions outlined in the Boot Virus Clean Wizard - 2 window.
4. When you are finished, click the Finish button.

{button ,AL(`How do I remove boot sector viruses?',0,`',`')} Related Topics

Boot Wizard Page 1 - Click on the area you would like more information on.

{button ,AL(`Boot Wizard;How do I remove boot sector viruses?',0,`',`')} Related Topics

Boot Wizard Page 2 - Click on the area you would like more information on.



{button ,AL(`Boot Wizard;Boot Wizard Page 1;How do I remove boot sector viruses?',0,`',`')} Related Topics

Clean Wizard

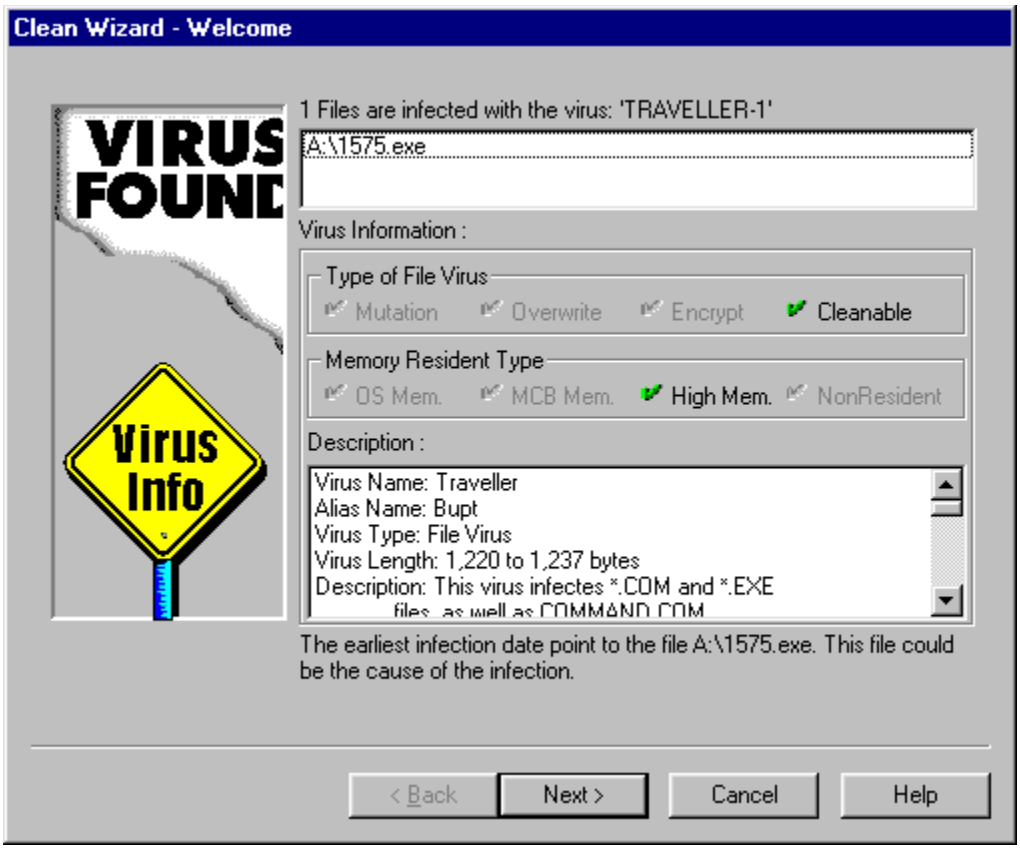
When you install PC-cillin II, you are automatically alerted if your system is infected with a virus, or there are any changes that could indicate the presence of an unknown virus. Viruses spread throughout your system through program files, system files, and startup boot disk records.

When PC-cillin II detects a virus, you are presented with a message box informing you that a virus was found, and the Clean Page window appears on your desktop. The Clean Page window allows you to clean, delete, and rename infected files using the "Clean Wizard" or the Clean, Delete and Rename command buttons.

PC-cillin II's Clean Wizard is designed for those of us who have never dealt with a computer virus before. The Clean Wizard steps you through the entire process of cleaning and removing viruses from your system in the safest method possible.

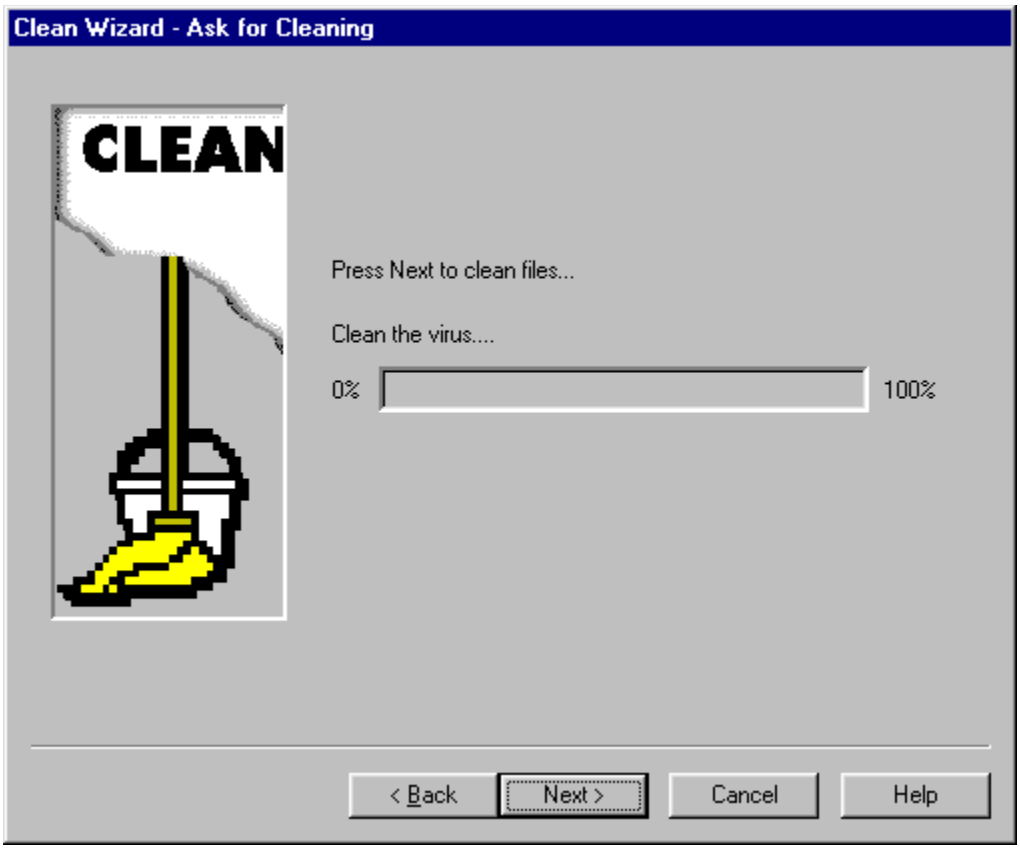
{button ,AL(`Clean Page;Clean Wizard - Ask For Cleaning;Clean Wizard - Done;Clean Wizard - Floppy;Clean Wizard - Scan Disk;Clean Wizard - Send E-Mail;Clean Wizard - Welcome;Cleaning Mutation Viruses;Cleaning virus infected files;How do I clean an infected file?;Virus Cleaner',0,`',`')} Related Topics

Clean Wizard - Welcome - Click on the area you would like more information on.



{button ,AL(`Clean Page;Clean Wizard',0,`',`')} Related Topics

Clean Wizard - Ask For Cleaning - Click on the area you would like more information on.



{button ,AL(`Clean Page;Clean Wizard',0,`',`')} Related Topics

Clean Wizard - Send E-Mail - Click on the area you would like more information on.

{button ,AL(`Clean Wizard;How do I print an E-Mail message?;How do I send an E-Mail message?',0,`',`')} Related Topics

How do I send an E-Mail message?

When you use PC-cillin II's Clean Wizard to remove detected viruses, you can send an e-mail message to anyone you share files with. This is a preventative measure to keep from re-infecting everyone's computer with the same virus.

To send an e-mail message:

1. Click the Send E-Mail button in the Clean Wizard - Send E-Mail window. The Choose Profile dialog box appears.
2. To accept the MS Exchange default setting, click the OK button. To choose another profile button, click the New button.

{button ,AL(`Clean Wizard - Send E-Mail',0,`',`')} Related Topics

How do I print an E-Mail message?

When you use PC-cillin II's Clean Wizard to remove detected viruses, you have an opportunity to print the e-mail message and provide a copy for anyone you share files with. This is a preventative measure to keep from re-infecting everyone's computer with the same virus.

To print an e-mail message:

1. Click the Print It button in the Clean Wizard - Send E-Mail window. The Print dialog box appears.
2. Choose the printer and select the number of copies you want to print.
3. Click the OK button to print the message.

{button ,AL(`Clean Wizard - Send E-Mail',0,`',`')} Related Topics

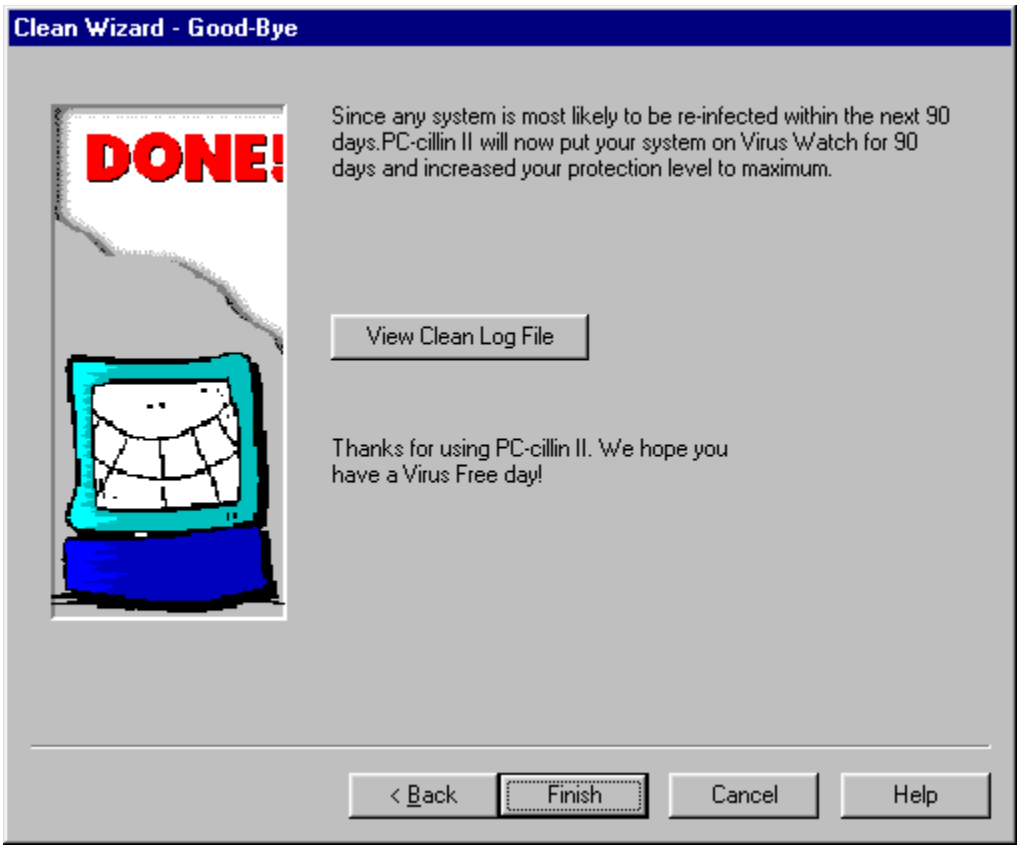
Clean Wizard - Scan Disk - Click on the area you would like more information on.

{button ,AL(`Clean Page;Clean Wizard',0,`',`')} Related Topics

Clean Wizard - Floppy - Click on the area you would like more information on.

{button ,AL(`Clean Page;Clean Wizard',0,`',`')} Related Topics

Clean Wizard - Done - Click on the area you would like more information on.



{button ,AL(`Clean Page;Clean Wizard',0,`',`')} Related Topics

How do I view a clean log file?

The Clean Wizard - Good Bye window gives you an opportunity to view, save and print a log of viruses cleaned from your computer.

To view a clean log file:

1. Click the View Clean Log File button in the Clean Wizard - Good Bye window. A copy of the report appears on your desktop displaying the name(s), date and time the virus(es) were cleaned.
2. To print or save the report, choose the desired option from the File menu.

{button ,AL(`Clean Wizard - Done',0,`',`')} Related Topics

Dealing with Uncleanable Viruses

Processing an uncleanable virus:

1. Choose the **Clean Wizard** button from the Clean tab. The Ask for Cleaning window appears.
2. To move onto the Send E-mail window, click the **Next** button. Otherwise, to deal with the virus immediately, click on the **Enter the Virus Lab Now** button in the middle of the window.
3. The Check-Up Center in the Internet Virus Lab opens. Instructions on what to do with the uncleanable virus will be provided. Mostly, this entails sending TouchStone the virus using the Virus Doctor window.
4. Use the Virus Doctor window to upload the virus to TouchStone's Virus Doctor staff (for more information, see Internet Virus Doctor). If there are multiple viruses, they will be uploaded in a single batch, meaning you will not have to repeat this process for each one.

WARNING! There are special conditions having to do with sending a batch. For more information, see Warning Messages During the Send Process.

Internet Virus Lab

The Internet Virus Lab uses a built-in ActiveX browser to give you up-to-the-minute virus news and information, virus outbreak alerts, and expert virus analysis. You no longer have to rely on word-of-mouth or computer magazines to find out about the newest viruses to hit the public. The Internet Virus Lab gives you accurate information on all the latest outbreaks as well as details on over 6,000 viruses.

Plus, the Internet Virus Lab is staffed 24 hours a day by a highly trained team of experts, who are there for you whenever you need help.

Accessing the Internet Virus Lab

There are two ways to access the Virus Lab: first, the **Virus Lab** button located in the Smart Monitor; second, Internet Virus Lab tab on the main window.

This tab contains an ActiveX module that acts as an Internet browser.

The appearance of this window varies as it is updated, but the Virus Lab should have a similar look and feel as the above example.

Connection Status

When you choose the Internet Virus Lab tab, PC-cillin II automatically brings up an Internet dialup connection dialog box.

In the upper right of the tab, a status bar displays the connection status similar to how Netscape and Internet Explorer work. When you select a file to be downloaded, a standard Windows 95 dialog box prompts you for a location where you want the file placed. During a download, a progress bar displays how far along the download is.

Toolbar

In the upper left, a browser toolbar lets you move back and forth through the web site. Also, the toolbar contains the following controls:

- **Back**: Moves back a page.
- **Forward**: Moves forward a page.
- **Home**: Returns to the home page. If you've gone several levels deep and you just want to get back to the starting point, use this button.
- **Reload:** Refreshes current page.
- **Print:** Prints current page. Reading on-line can strain even the best pair of eyes. If you want a hard copy, use this button to print the current page.
- **Stop:** Stops loading current page. This is useful if, for some reason, it's taking a really long time for a page or graphic to load.

{button ,AL(`Check-Up Center;File Downloads;Product News;Virus News',0,`',`')} Related Topics

Virus News

You can get the latest news and information on all the latest virus alerts by clicking on this link. The Virus News page connects to a monthly newsletter called Virus News Watch that contains front line news and information for the war against computer viruses. The newsletter is managed by TouchStone Software.

File Downloads

Through this link, you can receive program updates, patches, and new virus pattern files. The Program Update page has a table of files that you can download. The table lists each file's name, date, size, and description for easy identification.

If you are after an update to your virus pattern file, look for a file called "tsvpn" followed by a three-digit extension, which is the version of the file. The version numbers are sequential, meaning tsvpn.202 is newer than tsvpn.178.

Also, some files are self-extracting or self-installing. This means that when you download the file, you need to copy it to the PC-cillin II folder, then run extraction or installation process. You can do this through the Run command in the Start menu or by double-clicking on the file in Windows Explorer (or File Manager).

To download a file, click on its name, which is a link. The download will then commence. If you are downloading a self-extracting or self-installing file, you will need to provide a destination directory before the file is actually transmitted.

Be advised that depending on the speed of your modem or Internet connection and the size of the file, your download time may vary substantially.

Product News

Use this link to find out about the latest news on PC-cillin II.

Check-Up Center

The Check-Up Center verifies that you have the most recent versions of both the main PC-cillin II program and its virus pattern file. If you don't, the Check-Up Center advises you how to download the proper update(s).

The Check-Up Center also explains what to do in the event PC-cillin II discovers an uncleanable virus on your computer.

Exceeding File Size Upload

The upload to the Virus Doctor has a 2Mb capacity. If you are sending one or more viruses that exceed this size constraint, you will receive a warning message.

In this case, if you are sending multiple viruses, perhaps you can subtract several to get below the 2Mb limit. If you are transmitting a single 2Mb file, send a message to the Virus Doctor and we will make arrangements to get the file another way.

Not Enough Space Available

The best way to describe this error is to think of it in terms of a space account with a credit limit of 2Mb. If you send viruses to the Virus Doctor, your account is debited that amount of space. For example, you send 1Mb worth of viruses, you have 1Mb of space left in your account.

You will receive this message if you do anything that threatens to exceed your 2Mb account limit, like uploading more viruses.

There are several ways to avoid this problem. First, retrieve viruses/files that have been processed by the Virus Doctor and are waiting for you. Second, be aware of the size of the batch of viruses/files that you are uploading. If you send nearly 2Mb worth of viruses then soon thereafter try to upload another big batch, you'll get this message.

Remember, the Virus Doctor will attempt to process your viruses within three (3) hours, so be sure to check back in that time frame.

Internet Virus Doctor

If you ever find a virus that you just can't clean or get rid of, our experts will take care of it for you. You can automatically upload any infected files from your computer to TouchStone's Virus Doctor. We'll analyze the file(s) and respond within three hours. It's the only anti-virus solution that gives you personalized virus protection.

You can access the Virus Doctor through the Virus Doctor tab on the main window.

Entering a Message

Using the Message Box, you can relay any notes or information about the nature of an infection to our staff. Your name and e-mail address are included as well as the program version of PC-cillin II, the version of the virus pattern file (VPF), and the date/time that you opened the Virus Doctor tab.

Attaching Files

If PC-cillin II detects an uncleanable file, or if you just have a problematic file involving a virus infection, you can forward it to our staff for analysis. To do so, use the **Attach File** button to bring up a standard Windows open dialog box. Choose the file(s) you want to send.

Once you have selected the proper file, its name will appear in the Attached Files box on the right side of the tab.

You can remove a file(s) from the attached files list. Highlight the file(s) that you want to take off, then click on the **Remove File** button.

Sending a Message to the Virus Doctor

Once you have entered the message you want and attached the proper file(s), you can upload the message to the Virus Doctor by clicking on the **Send to Doctor** button.

Warning Messages During the Send Process

There are special conditions that exist when sending things to the Virus Doctor.

Exceeding File Size Upload
Not Enough Space Available

Receiving a Response from the Virus Doctor

To check and see if you have received a response from our staff, click on the **Get From Doctor** button. PC-cillin II automatically determines whether or not there is a message back to you and, if there is, downloads it.

Virus Scanner

Networking between computers is becoming more and more common, and sharing files downloaded from the Internet, the BBS or from a floppy diskette onto your computer increasingly exposes you to the risk of virus infection. To ensure that your computer remains virus-free, all files should be periodically scanned for viruses.

PC-cillin II's virus scanner permits you to check your local hard and floppy drive(s) for viruses at any time (using the manual scan feature) or at preset times (using the prescheduled scan feature). If you use floppy disks, are on a network or server of any kind, or let other people use your system, you are susceptible to viruses, some of which can destroy ALL the data on your system.

{button ,AL(`How do I scan for viruses?;Scheduled Scans;Scan Options Page;Scan Page;Virus Scanner Options',0,`',`')} Related Topics

Virus Scanner Options

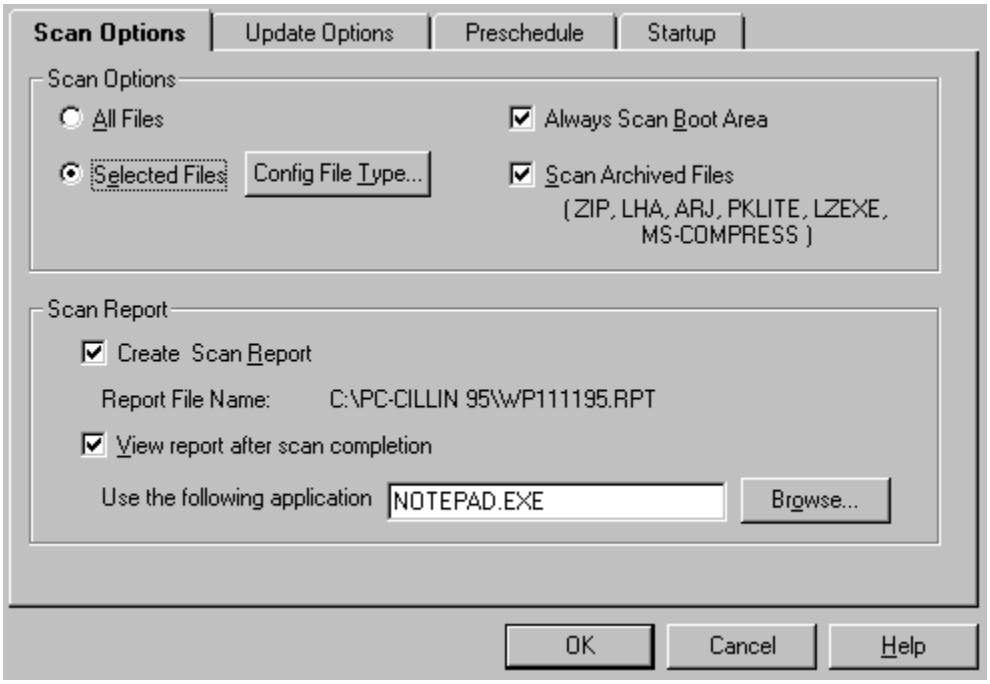
You can fine-tune the way PC-cillin II scans your system to increase system security, reduce scanning time, and perform specific tasks. Certain options can be configured for the Virus Scanner--for example, you can:

- scan the partition table and boot sector of your PC
- scan archived/compressed files
- scan all files
- scan specific files
- create a scan report
- view a scanned report
- select a word processor to view a report in

PC-cillin II's default settings scan the boot area, every file (including compressed files) on your computer, and generates a scan report automatically. However, you can modify these default settings to fit your needs.

{button ,AL(`How do I create a Scan Report;How do I scan specific files?;How do I select a word processor?;How do I view a Scan Report?;Scan Options Page;Scan Page',0,`',`')} Related Topics

Scan Options Page - Click on the area you would like more information on.



{button ,AL(`How do I add program file extensions?;How do I configure PC-cillin options?;How do I create a Scan Report?;How do I delete program file extensions?;How do I scan all files?;How do I scan compressed files?;How do I scan for viruses?;How do I scan specific files?;How do I scan the boot area?;How do I select a word processor?;How do I view a Scan Report;Virus Scanner Options',0,`',`')} Related Topics

How do I scan all files?

To scan all files:

1. Choose Scan Options from the Options menu.
2. Or, click the Main button located in either the Smart Monitor or Custom Monitor window. The Options dialog box appears.
3. By default, the Scan Options Tab is selected and the Scan Options page appears.
4. Select the All Files check box in the Scan Options group box.
5. To confirm your selection, click the OK button.

{button ,AL(`Scan Options Page;Virus Scanner Options',0,`',`')} Related Topics

How do I scan the boot area?

To scan the boot area:

1. Choose Scan Options from the Options menu.
2. Or, click the Main button located in either the Smart Monitor or Custom Monitor window. The Options dialog box appears.
3. By default, the Scan Options Tab is selected and the Scan Options page appears.
4. Select the Scan Archived Files check box in the Scan Options group box.
5. To confirm your selection, click the OK button.

{button ,AL(`Scan Options Page;Virus Scanner Options',0,`',`')} Related Topics

How do I scan compressed files?

To scan compressed files:

1. Choose Scan Options from the Options menu.
2. Or, click the Main button located in either the Smart Monitor or Custom Monitor window. The Options dialog box appears.
3. By default, the Scan Options Tab is selected and the Scan Options page appears.
4. Select the Scan Archived Files check box in the Scan Options group box.
5. To confirm your selection, click the OK button.

{button ,AL(`Scan Options Page;Virus Scanner Options',0,`',`')} Related Topics

How do I scan specific files?

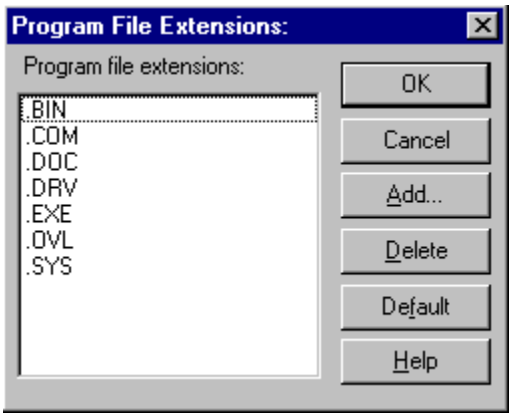
By default, PC-cillin II scans .BIN, .COM, .DOC, .DRV, .EXE, .OVL, and .SYS files. You can use the Program File Extensions dialog box to add, delete or accept the default program file type extensions.

To scan specific files:

1. Choose Scan Options from the Options menu.
2. Or, click the Main button located in either the Smart Monitor or Custom Monitor window. The Options dialog box appears.
3. By default, the Scan Options Tab is selected and the Scan Options page appears.
4. Select the Selected Files radio button and click the Config File Type button in the Scan Options group box. The Program File Extensions dialog box appears.
5. Add or delete the program file types you want to scan.
6. Click the OK button to confirm your selection(s). Control returns to the Scan Options page.

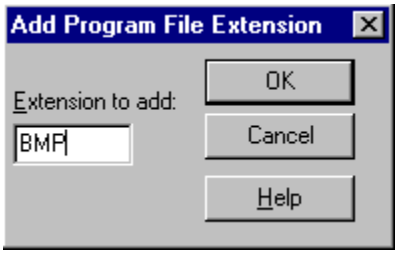
{button ,AL(`How do I add program file extensions?;How do I delete program file extensions?;Scan Options Page;Virus Scanner Options',0,`',`')} Related Topics

Program File Extension Dialog - Click on the area you would like more information on.



{button ,AL(`How do I add program file extensions?;How do I delete program file extensions?;Scan Options Page',0,`',`')} Related Topics

Add File Extension Dialog - Click on the area you would like more information on.



{button ,AL(`How do I add program file extensions?;How do I delete program file extensions?;Program File Extension Dialog;Scan Options Page',0,`',`')} Related Topics

How do I add program file extensions?

To add program file extensions:

1. Choose Scan Options from the Options menu.
2. Or, click the Main button located in either the Smart Monitor or Custom Monitor window. The Options dialog box appears.
3. By default, the Scan Options Tab is selected and the Scan Options page appears.
4. Select the Selected Files radio button and click the Config File Type button in the Scan Options group box. The Program File Extensions dialog box appears.
5. Click the Add button. The Add Program File Extension dialog appears.
6. Type the 3 character file extension in the **Extension to add** text box.
7. To abort adding the program file type, click the Cancel button. To add the program file type, click the OK button. Control returns to the Program File Extension dialog box.
8. Click the OK button to confirm your selections.

{button ,AL(`Scan Options Page;Virus Scanner Options',0,`',`')} Related Topics

How do I delete program file extensions?

To delete program file extensions:

1. Choose Scan Options from the Options menu.
2. Or, click the Main button located in either the Smart Monitor or Custom Monitor window. The Options dialog box appears.
3. By default, the Scan Options Tab is selected and the Scan Options page appears.
4. Select the Selected Files radio button and click the Config File Type button in the Scan Options group box. The Program File Extensions dialog box appears.
5. Select the file type extension(s) you want to delete.
6. Click the Delete button. The selected file types are removed from the list.
7. To confirm the deletion, click the OK button. Control returns to the Scan Options page.

Note: The next time PC-cillin II scans your computer, the deleted program file extension is excluded from the scanning session. There must be at least one extension present for the scan to operate.

{button ,AL(`Scan Options Page;Virus Scanner Options',0,`',`')} Related Topics

How do I create a Scan Report?

When PC-cillin II detects a virus on your computer, or in your folders/sub-folders, the scan report automatically appears on your desktop where you can view the results instantly. However, PC-cillin II allows you to view the scan report of a virus-free scanning session at your convenience, using your favorite word processing application.

Scan reports provide you with a hard copy reference you can use to keep track of viruses your system becomes infected with. When PC-cillin II detects a virus on your computer, or in your files, PC-cillin II automatically creates a scan report each time you scan your system. PC-cillin II also gives you the option of turning this feature off.

The scan report provides you with the following information:

- Date/Time of scan
- Drive(s) scanned
- Number of files checked
- Number of infected files found

To create a scan report:

1. Choose Scan Options from the Options menu. The Options dialog box appears.
2. To generate a scan report every time you perform a scanning session, select the Create Report check box.
3. To turn the Create Report option off, select the Create Report check box again.

   Note: When the Create Report option is selected, every time you scan your system, a report is generated. The filename for the generated report appears in the Scan Report group box.

{button ,AL(`How do I configure PC-cillin options?;How do I select a word processor?;How do I view a Scan Report?;Scan Options Page;Virus Scanner Options',0,`',`')} Related Topics

How do I select a word processor?

PC-cillin II allows you to choose which word processing application you want to view a scan report in. By default, NOTEPAD.EXE is selected.

To select a word processor:

1. Choose Scan Options from the Options menu.
2. Or, click the Options command button in the Scan Page window. The Scan Options page appears.
3. Select the Create Scan Report check box in the Scan Report group box.
4. Deselect the **View report after scan completion** check box in the Scan Report group box.
5. Type or select the word processing application you want in the **Use the following Application** text box. By default, NOTEPAD.EXE is selected.
6. To choose another application, click the Browse command button and select the application you want.
7. To confirm your selections, click the OK button.
8. After you have completed a scan session, launch the word processing application you selected.
9. Choose Open from the File menu.
10. Open the scan report (Report File Name) filename you want. For more information, refer to your word processing documentation.

    Warning! If PC-cillin II detects a virus, and the Scan Report group box options are selected, PC-cillin II launches the selected word processing application automatically, and displays the report on your desktop.

{button ,AL(`How do I create a Scan Report;Scan Options Page;How do I view a Scan Report;Virus Scanner Options',0,`',`')}
Related Topics

How do I view a Scan Report?

To view the results of a scanning session, the **Create Scan Report** and **View report after scan completion** check boxes must be selected in the Scan Report group box in the Scan Options page. When PC-cillin II detects a virus, you have the option of viewing the report instantly, or at a later time when it's convenient for you.

To view a scan report:

1. Choose Scan Options from the Options menu.
2. Or, click the Options command button in the Scan Page window. The Scan Options page appears.
3. To view a scan report instantly, select the **View report after scan completion** check box in the Scan Report group box.
4. To view a scan report at your convenience, deselect the **View report after scan completion** check box in the Scan Report group box.
5. To confirm your selections, click the OK command button.

   Note: If you selected the **View report after scan completion** check box, the next time a virus is detected, the scan report automatically appears on your desktop.

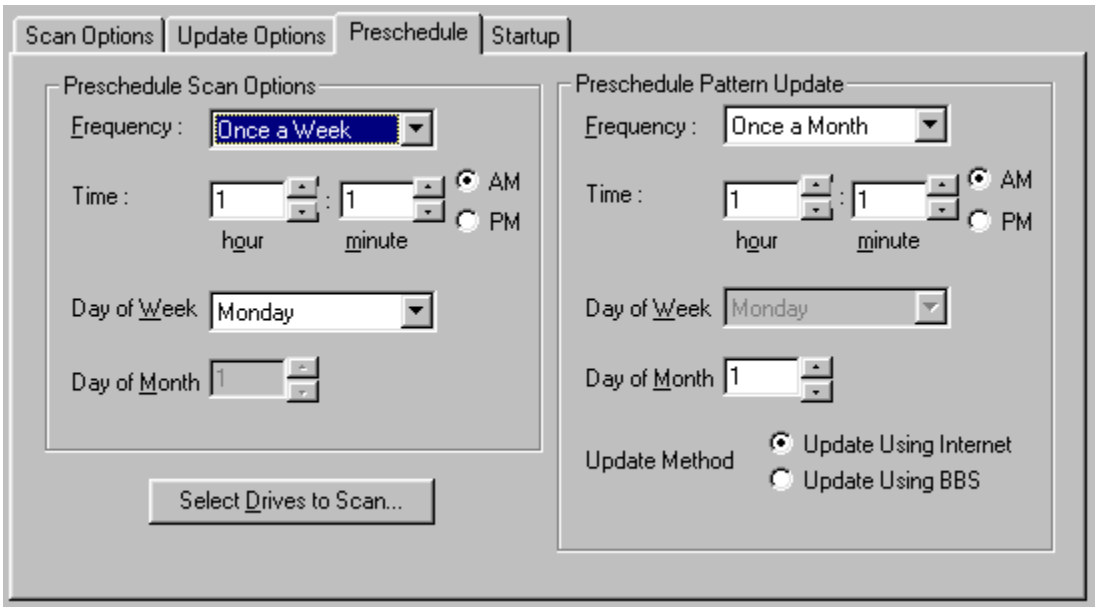
Scheduled Scans

PC-cillin II's Prescheduled Scan feature allows you to automate your scanning activities by selecting the scan destination, types of files, and the date, time and frequency for automatic scanning on your computer.

You can schedule events that run unattended on specific dates and times or at periodic intervals. If you are using the computer when the scheduled scan begins, it runs in the background so that you do not have to stop working.

{button ,AL(`How do I set a scheduled scan?;Preschedule Page',0,`',`')} Related Topics

Preschedule Page - Click on the area you would like more information on.



{button ,AL(`How do I set a scheduled scan?;Scheduled Scans',0,`',`')} Related Topics

How do I set a scheduled scan?

You can schedule events that run unattended on specific dates and times, or at periodic intervals. If you are using the computer when the scheduled scan begins, it runs in the background so that you do not have to stop working.

To set a scheduled scan:

1. Choose Preschedule Options from the Options menu.
2. Or, from the Scan Page window, click the Options command button. The Options dialog box appears.
3. Click the Preschedule Tab. The Preschedule page appears.
4. Type or select how often you want the scan to occur in the Frequency drop-down list box.
5. Type in or click the arrow button(s) to select the time in the hour/minute text boxes.
6. To scan on a weekly basis, select the day of the week in the Day of Month text box.
7. Or, to scan on a monthly basis, select the day of the week in the Day of Month text box.
8. Click the Select Drives to Scan command button. The PreSchedule Browser dialog box appears.
9. Choose the drive(s) you want to scan.
10. To accept the selections made, click the OK command button. Control returns to the Preschedule page.
11. To complete the scheduled event, click the OK command button in the Preschedule page.

    Note: Preschedule Options must be set and active before scheduled scans can run.

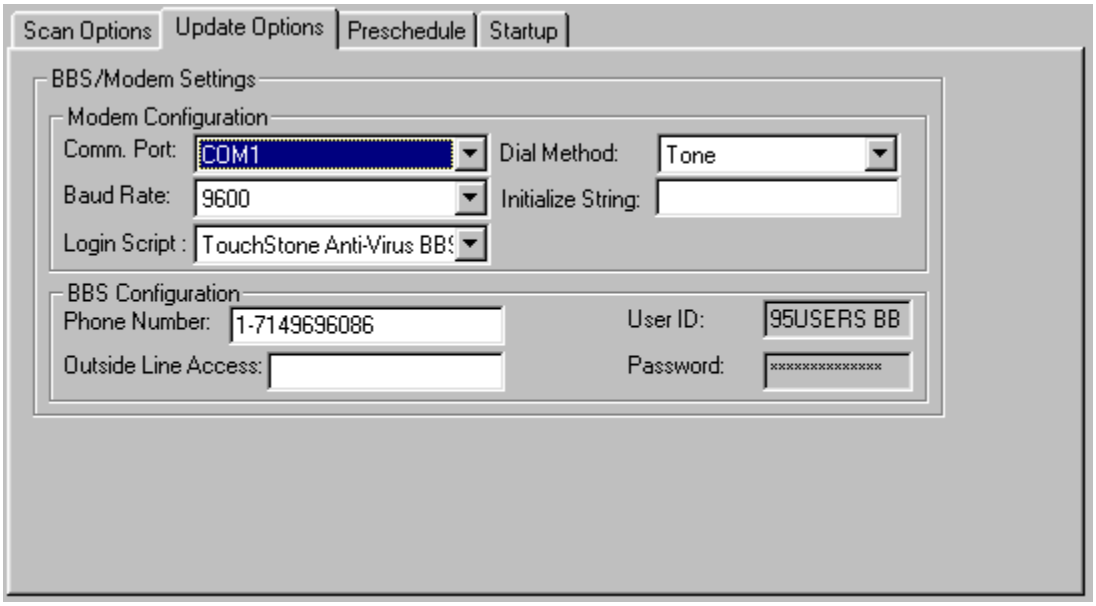
{button ,AL(`Preschedule Page;Scheduled Scans',0,`',`')} Related Topics

Update (Pattern) Options

If you have a modem installed on your computer and have access to a telephone line, PC-cillin II's modem setup utility lets you automatically download the latest virus pattern file from PC-cillin II's BBS or WWW server on the Internet. After you configure your modem for the first time, subsequent updates only require one mouse button click. However, before you can download the latest virus pattern file, you must register your copy of PC-cillin II and make sure your modem is properly configured.

By default, PC-cillin II includes the Internet, BBS/Modem and BBS Configuration settings along with the necessary User IDs and Passwords required in order to access PC-cillin II's BBS or World Wide Web site. PC-cillin II allows you to change the Comm Port, Baud Rate, Dial Method and Outside Line Access options for your modem through the Update Options Page.

Update Options Page - Click on the area you would like more information on.



{button ,AL(`How do I access the BBS or WWW site?;How do I change BBS/Modem settings?;Update Pattern Options',0,`',`')}
Related Topics

How do I change BBS/Modem settings?

PC-cillin II allows you to change the Comm Port, Baud Rate, Dial Method and Outside Line Access options for your modem. By default, PC-cillin II includes the Internet, BBS/Modem and BBS Configuration settings, along with the necessary User IDs and Passwords required in order to access PC-cillin II's BBS or World Wide Web site, so you do not need to worry about setting these options, it's done for you.

To change modem settings:

1. Choose Update Pattern Options from the Options menu.
2. Or, choose the Update Options tab from the Options dialog box. The Update Options page appears.
3. Select the Comm Port, Baud Rate, and Dial Method settings appropriate for your fax modem.
4. If necessary, enter the number required to access an outside line (i.e., 9).

{button ,AL(`Update Options Page;Update Pattern Options',0,`',`')} Related Topics

How do I access the BBS or Internet site?

If you have a modem installed on your computer and have access to a telephone line, PC-cillin II's modem setup utility lets you automatically download the latest virus pattern file from PC-cillin II's BBS or Internet site.

To access the BBS or Internet site:

Choose Update Pattern Options from the Options menu. The Update Options page appears.

Settings for the BBS are:

8 data bits, 1 stop bit, no parity

To contact PC-cillin II's BBS, dial

714-969-6086
408-255-2054

Service Providers That Work

PC-cillin II should work with any browser that is capable of supporting the Windows 95 32-bit TCP/IP protocol stacks for the single button download.

For the Internet/Email Monitor option, PC-cillin II works with the following browsers:

In-Box - Microsoft Exchange for Windows 95
Lotus cc:Mail
cc:Mobil
Netscape
Internet Explorer for Windows 95
WS_FTP32
Forte Agent
Telnet
FTP
NCSA Mosaic
Spry Mosaic
Air Mosaic
NetCruiser

Startup Protection

The initial level of protection against virus attacks are special scans that occur each time your computer starts up. These scans catch viruses that infect files and boot records your computer uses to prepare itself for work. Startup scans are a vital part of virus protection because they make sure your computer is virus-free every time you start up.

{button ,AL(`Startup Options;Startup Page',0,`',`')} Related Topics

Startup Options

Certain options can be configured for your computer during Startup operations. These options include:

System Startup: Scan Memory - Scans memory for viruses whenever your system starts up.

Always Scan Boot Area - Scans the boot and partition table whenever your system starts up.

Startup Options: Load PCSCAN into the AUTOEXEC.BAT - Inserts a load command in your AUTOEXEC.BAT file that tells your computer to perform a scan every time you boot up your system. This is not a terminate-and-stay resident (TSR) program. We recommend choosing this option to make sure you boot into a virus-free environment.

Dock Program into Taskbar - Loads the program into the taskbar every time you enter Windows 95. PC-cillin II's application icon can be seen in the lower right hand corner of the taskbar.

Monitor Mode
Provides you with two options for monitoring your system: Smart Monitor and Custom Monitor. Select the option you want and click the preferred Setup command button to specify how PC-cillin II monitors and protects your computer from viruses. To monitor every file you access on your computer, select the Monitor All Files Accessed check box.

Executable File Modification Deny
Eliminates the possibility of writing a virus infected file into a particular folder/sub-folder. To deny access to a specified folder/sub-folder, select the Selected Folder command button to designate which folder/sub-folder you want to deny access to.

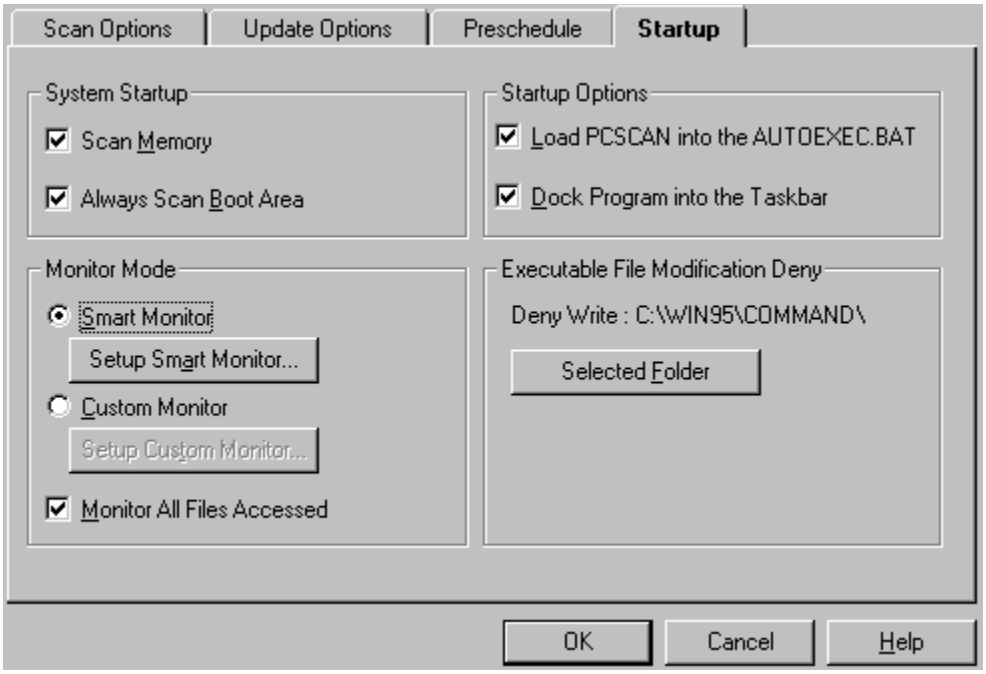
OK Button
Closes the Startup window and returns control to the previous window saving any selections made. The next time you boot your computer, PC-cillin II activates the selections made in the Startup window.

Cancel Button
Closes the Startup window and returns control to the previous window without making any changes.

Help Button
Displays the online Help topic for this window.

{button ,AL(`How do I change startup protection?;How do I deny write capabilities?;How do I dock PC-cillin II?;Startup Page;Startup Protection',0,`',`')} Related Topics

Startup Page - Click on the area you would like more information on.



{button ,AL(`How do I change startup protection?;How do I deny write capabilities?;How do I dock PC-cillin II?;Startup Options;Startup Protection',0,`',`')} Related Topics

How do I change startup protection?

To modify PC-cillin II's startup protection to fit your needs, follow the steps outlined below.

To change startup protection:

1. Choose Startup Options from the Options menu. The Startup page appears.
2. To scan your systems memory every time the program loads, select the Scan Memory check box.
3. To perform a scan every time you boot up your system, select the Load PCSCAN into the AUTOEXEC.BAT check box.
4. To automatically load PC-cillin II into the taskbar, select the Dock Program into Taskbar check box.
5. Choose the Monitor Mode for which you want PC-cillin II to scan your computer (Smart Monitor or Custom Monitor).
6. To deny write capabilities (access) to a specific folder/sub-folder, select the folder/sub-folder you want.
7. When you are finished selecting the startup options you want, click the OK button. The next time you access the program, the options you selected take effect.

{button ,AL(`Startup Options;Startup Page;Startup Protection',0,`',`')} Related Topics

How do I dock PC-cillin II?

Docking PC-cillin II's application window allows you to hide the program from your view while running in the background. Even though you cannot see the Smart/Custom Monitor window, when the Dock to Taskbar option is enabled (turned on), you can relax knowing that PC-cillin II is running in the background continuously monitoring your system for viruses.

To dock PC-cillin II:

1. Choose Scan Options from the Options menu. The Options dialog box appears.
2. Select the Startup Tab. The Startup page appears.
3. Select the **Dock Program into Taskbar** check box in the Startup Options group box.
4. To confirm your selection, click the OK button.
   The next time you launch PC-cillin II, the program appears as an icon on the taskbar.

{button ,AL(`Startup Options;Startup Page;Startup Protection',0,`',`')} Related Topics

How do I deny write capabilities?

To eliminate the possibility of writing a virus infected file into a particular folder or sub-folder, you need to enable the deny write function.

To deny write capabilities:

1. Choose Startup Options from the Options menu. The Startup Page appears.
2. Click the Select Folder command button. The Browse for Computer dialog box appears.
3. Select the folder and/or sub-folder you want to deny access to. For more information on how to select a folder, refer to your Windows 95 documentation.
4. Click the OK button. Control returns to the Startup page.

   The folder you selected appears in the Deny Write area in the Executable File Modification Deny group box.

{button ,AL(`Startup Options;Startup Page;Startup Protection',0,`',`')} Related Topics

Virus Threats

Since a major portion of modern day information is stored and accessed through computers, new virus threats are constantly emerging. Network connections, file sharing and peer-to-peer transfers in Windows 95 bring a variety of infection possibilities. The emergence of on-line viruses, especially those lurking throughout the Internet, has created an increased threat of infection for any system with a modem. If not detected, these new virus strains can infect and destroy an entire network in less than an hour.

If you use a PC to exchange programs with other people, or you access computer networks over telephone/modem lines, you are at risk of becoming infected with a computer virus.
PC-cillin II monitors all data that comes through a modem line connection to filter out the thousands of viruses lurking throughout the Internet and commercial on-line services.

{button ,AL(`Known viruses;Types of viruses;Unknown viruses;What is a virus?',0,`',`')} Related Topics

Types of viruses

Boot Sector Viruses

The boot sector is the portion of a hard disk that controls how your operating system starts when you turn on your computer. A boot sector virus replaces the disk's original boot sector with its own, and loads the virus into memory. Once in memory, the virus can spread to other disks which helps it avoid detection against prevention programs.

Parasitic Viruses

A parasitic virus hides in memory and adds virus code to files that run programs, so the virus is activated whenever you run the program. When the virus is activated, it spreads to other program files that act like parasites to the MS-DOS interrupt functions. This type of virus literally takes control of low-level DOS functions. Generic viruses attach themselves to "system-level" executable files and thus gets executed each time the infected file is executed.

Stealth Viruses

Stealth viruses modify themselves to avoid detection by most anti-virus scanning programs; they may also be able to avoid DOS interrupt vectors. This is the newest and most difficult virus to detect. Just like a biological virus, a computer virus must replicate itself to survive. Therefore, every virus strain has some method of replicating itself.

Computer viruses fall into two categories--known viruses and unknown viruses. PC-cillin II detects and removes both known and unknown viruses on your computer.

{button ,AL(`How do I view virus information?;How is a virus activated?;How is a virus spread?;How PC-cillin II Protects You;How PC-cillin II Warns You;Is my computer protected against viruses?;Known viruses;Unknown viruses;Virus Information;What is a virus?;What is the life cycle of a computer virus?',0,`',`')} Related Topics

Known viruses

A known virus is one that has been identified. Once identified, statistics about the virus are stored in a virus pattern file. When PC-cillin II scans your disks and files, it searches your files for these signatures. If a file is infected with one of these viruses, PC-cillin II walks you through the process of destroying it.

When a new virus is discovered, its virus signature must be added to the virus pattern file. For this reason, you should update your virus pattern file regularly (a new pattern file is available monthly). This added protection provides you with necessary data to catch all known viruses.

{button ,AL(`How PC-cillin II Protects You;How PC-cillin II Warns You;Types of viruses;Unknown viruses;Virus Information',0,`',`')}
Related Topics

Unknown viruses

An unknown virus is one that does not yet have a virus definition. PC-cillin II looks for programs that have been modified without your knowledge. PC-cillin II detects unknown viruses by constantly monitoring activity on your system for behaviors that viruses usually perform when replicating or attempting to damage your files. When a suspect activity is detected, PC-cillin II stops the program from running and initiates corrective action.

{button ,AL(`How PC-cillin II Protects You;How PC-cillin II Warns You;Types of viruses;Known viruses;Virus Information',0,`',`')}
Related Topics

What is a virus?

Viruses are programs designed to replicate and damage your computer system without your knowledge or permission. A virus may attach itself to another program or to the partition table and boot sector of your hard disk. A virus will wait for a certain event before executing its programmed routine. Some viruses are harmless, but others are capable of destroying your hard disk and all the data contained in it.

A virus may also be categorized by the type of damage it does. Some so-called "viruses" are actually harmless; they may only show a message on the screen or change the colors. A malicious virus, on the other hand, will destroy data once it is activated. It may format your hard drive or secretly change the values in a database file.

{button ,AL(`How do I view virus information?;Types of viruses;Virus Threats',0,`',`')} Related Topics

How is a virus activated?

One characteristic of most successful viruses is that they do not immediately begin destroying data. This behavior, called "dormancy," is necessary for long-term survival. While these viruses are dormant, they scan events, such as the system date, or user behavior (such as the number of keystrokes entered) and then activate when certain conditions are met. This set of conditions is called the "catalyst."

Avoiding the catalyst is not a good way to avoid a virus. Even if you manage to dodge it once, you will likely have the same conditions again in the future. You still need to find and remove the virus.

{button ,AL(`Types of viruses;Virus Threats',0,`',`')} Related Topics

How is a virus spread?

The two main transmission mediums for viruses are:

- electronic networks (i.e, Bulletin Board Systems)
- files and software exchanged on disk or tape

Be on alert anytime you use a modem to download files or put new software or files on your computer. Always have PC-cillin II active to scan the new files for viruses.

{button ,AL(`Types of viruses;Virus Threats',0,`',`')} Related Topics

What is the life cycle of a computer virus?

There are three phases in the life cycle of computer viruses:

- transmission
- replication
- manipulation

In the transmission stage, a virus infects a file in the computer. In the replication stage, the virus copies itself within your system. In the manipulation stage, the virus achieves it's final goal—often destroying data. Unless the virus is removed, it continues to infect other files and possibly damage all the information on your hard disk.

{button ,AL(`Types of viruses;Virus Threats',0,`',`')} Related Topics

Is my computer protected against viruses?

When you install PC-cillin II and accept the preset (default) options, your computer is safe. As part of the installation, your startup disk is scanned for viruses. After installation, the Smart Monitor's smart protection features provide you with constant protection while you work. The Smart Monitor checks programs for viruses when they are being used. If a virus is found, PC-cillin II's "Clean Wizard" walks you through the removal process.

{button ,AL(`How PC-cillin II Protects You',0,`',`')} Related Topics

Can I keep my computer virus-free?

To keep your system virus-free, we recommend the following:

- To prevent viruses from entering your computer, make sure PC-cillin II is always loaded and Startup scans are enabled.
- If you regularly download data through the Internet, a BBS or online service (i.e., CompuServe), be sure PC-cillin II is loaded on a daily basis; otherwise, scan all hard disk drives at least once a week to verify they are virus-free.
- Scan all new files and floppy diskettes before the first use. Drag-and-drop a folder or floppy disk icon on any PC-cillin II main program window (e.g., Scan Page, Clean Page, etc.).
- Create an emergency rescue disk, which is used to recover damaged hard disks.
- Update your virus pattern file regularly to ensure you are protected against newly discovered viruses.

{button ,AL(`How do I create a Clean Boot Disk?;How do I create a Rescue Disk?;How do I enable PC-cillin protection?;Startup Protection;Updating PC-cillin II regularly;Virus Threats',0,`',`')} Related Topics

How do I enable PC-cillin protection?

PC-cillin protection is automatically enabled every time the program is run.

To enable PC-cillin II protection:

1. Choose Programs, the PC-cillin II group, and PC-cillin II from the Start menu.
2. Release the mouse button to launch the program. By default, PC-cillin II automatically docks into the taskbar.
3. To open PC-cillin II's application window, double-click the program icon.
4. Or, using the left mouse button, double-click PC-cillin II's application icon on the taskbar.
5. Or, using the right mouse button, right-click the program icon and choose Open PC-cillin II or Show Monitor.
   When you choose Open PC-cillin II, the main program window appears. When you choose Show Monitor, the Smart Monitor window appears.

{button ,AL(`How PC-cillin II Protects You;Virus Monitor',0,`',`')} Related Topics

How do I configure PC-cillin options?

PC-cillin options can be configured by following the steps below:

1. Bring up PC-cillin II's main program window.
2. Choose Options from the menu bar. The Options dialog box appears.
3. Click on the Tab for the feature you want to configure. The applicable page for the Tab you selected appears.
4. To switch to another option, simply click the desired Tab.

{button ,AL(`Custom Monitor Window;Scan Options Page;Scheduled Scans;Startup Options;Update Pattern Options;Virus Scanner Options',0,`',`')} Related Topics

How do I create a Clean Boot Disk?

In DOS or Windows, create a clean boot disk that you can use if your system becomes infected. Before you create a clean boot disk, be sure your system is completely virus-free.

To create a clean boot disk:

1. Insert a blank floppy disk in selected target drive (A or B).
2. From the DOS command line (C:\>) format the disk by typing FORMAT A: /s/v/u. If the selected target drive is B, type **FORMAT B: /s/v/u**.

{button ,AL(`Can I keep my computer virus-free?',0,`',`')} Related Topics

How do I create an Emergency Rescue Disk?

Creating an emergency rescue disk is an important part of virus protection. It stores critical system information and the programs necessary to start your computer. A rescue disk is the only means to recover from certain types of boot viruses.

When you installed PC-cillin II, you were given an opportunity to create an emergency rescue disk. If you chose not to create one then, you can create one now. You need one high density floppy disk.

To create an emergency rescue disk:

1. Choose Programs, PC-cillin II, and Create Emergency Rescue Disk from the Start menu. The Create Emergency Rescue Disk dialog box appears.
2. Insert a blank high density diskette to selected target drive (A or B) and click Start. When the emergency rescue disk is successfully created, the Create Rescue Disk message box appears.
3. To complete the procedure, click the OK command button.
4. Label the disk to identify the computer for which it was created, along with the date the disk was made.
5. Write-protect the Emergency Rescue Disk and store it in a safe place.

{button ,AL(`Can I keep my computer virus-free?',0,`',`')} Related Topics

Why should I disable PC-cillin II protection?

There may be times when you will want to unload PC-cillin II from your computer. For example, you may want to unload the program if you experience any conflicts with another system or your system slows down from having too many windows open. However, remember that when you unload PC-cillin II from your computer, you eliminate your protection and increase your risk of acquiring a virus until the program is reloaded.

{button ,AL(`How do I remove PC-cillin II?;How do I unload PC-cillin II?',0,`',`')} Related Topics

How do I unload PC-cillin II?

There may be times when you will want to unload PC-cillin II from your computer. For example, you may want to unload the program if you experience any conflicts with another system, or your system slows down from having too many windows open. However, remember that when you unload PC-cillin II from your computer, you eliminate your protection, and increase your risk of acquiring a virus until you reload the program.

To unload PC-cillin II:

1. Right-click the mouse on PC-cillin II's icon on the taskbar, and choose **Unload PC-cillin II** from the pop-up menu.
2. Or, click the Unload button from the Smart Monitor or Custom Monitor window. The **Do you really want to exit PC-cillin II?** message box appears.
3. To abort exiting the program, click No. Control returns to PC-cillin II's main program window.
4. To continue and exit the program, click Yes.

{button ,AL(`Why should I disable PC-cillin protection?;How do I remove PC-cillin II?',0,`',`')} Related Topics

How do I remove PC-cillin II?

The Uninstall Program makes it easy for you to remove PC-cillin II from your computer. However, before you can remove PC-cillin II from your computer, you must turn the dock to taskbar option off, and unload the program.

To remove PC-cillin II:

1. Choose Settings, Control Panel from the Start menu.
2. Double-click the Add/Remove Programs icon. The Add/Remove Program Properties dialog box appears.
3. Select PC-cillin II and click the Remove command button.
4. Or, choose Programs, and PC-cillin II's Uninstall applet from the Start menu. The **Confirm File Deletion** message box appears.
5. To abort the operation, click the No button. To proceed with the removal of the application, click the Yes button. The **Remove Programs from your Computer** message box appears.
6. To complete the uninstall procedure, click the OK button. The uninstall program removes PC-cillin II from your system.

{button ,AL(`How do I change startup protection?;How do I unload PC-cillin II?',0,`',`')} Related Topics

What if I have a virus?

If you know that you have a virus, you can use PC-cillin's Virus Cleaner to remove the virus from your system. If the virus is in memory, you need to shut down your computer and boot from a clean boot disk.

{button ,AL(`Cleaning virus infected files;How PC-cillin II Protects You;How PC-cillin II Warns You;Virus Cleaner',0,`',`')} Related Topics

What if I suspect I have a virus?

If you suspect you have a virus but don't know for sure, you can run PC-cillin II's Virus Scanner to search for viruses. If a virus is found, PC-cillin's Virus Cleaner can be used to remove the virus from your system.

{button ,AL(`Can I keep my computer virus-free?;Determining When To Scan;Virus Scanner;Virus Threats',0,`',`')} Related Topics

What if a virus is found?

When PC-cillin II detects a virus, the virus name and the name of the infected file(s) appears in the Infected File Name text box in the Clean Page window.

PC-cillin II offers three ways to deal with viruses: clean, delete and rename the infected file(s). As you perform an action on a virus (using the Clean Wizard or the Clean, Delete or Rename command buttons), that virus is removed from the Scan Result-Infected File Name list. Thus, when you have deleted, renamed, or cleaned all the detected viruses, the list box will be empty.

{button ,AL(`Cleaning Mutation Viruses;Cleaning virus infected files;How do I remove a virus?;How do I view virus information?;How is a virus activated?;How is a virus spread?;How PC-cillin II Warns You;Virus Cleaner;Virus Information',0,`',`')} Related Topics

What if my computer won't start?

If your computer won't start, it is possible that it was infected by a virus. If it was caused by a virus, you can use PC-cillin II's Emergency Rescue Disk to recover, or you can use a clean boot disk to access your system, find the source, and eliminate it.

{button ,AL(`How do I create a Clean Boot Disk?;How do I create an Emergency Rescue Disk?;Is my computer protected against viruses?;Updating PC-cillin II regularly;What is the life cycle of a computer virus?',0,`',`')} Related Topics

Service and Support

The following support options are available:

Technical Support
BBS Support
CompuServe Support
Fax Back Support

Technical Support

TouchStone Software provides users support during the time period proven to be the most critical; for 90 days after the first service call or a maximum of 90 days from registration date. This support is available from 8:00 am to 5:00 pm Pacific Standard Time (PST) Monday through Friday for all currently published software products to all customers who have registered their products. Phone: (714) 374-2801. Fax: (714) 969-4444.

Out of Warranty Support

In a continuing effort to provide service to our customers, TouchStone Software offers support after the complimentary warranty period to users for any of their published software on a chargeable basis. Users have the option of calling (800) 859-1763 using their Visa/MasterCard/American Express to receive support at $2.00/min U.S. rate. Registration is recommended, but not required for chargeable service. Registered users may also use TouchStone's online services for support at no charge.

Extended Service Support

TouchStone Software is located in the Pacific Time Zone. Because users often require support after-hours/holidays/weekends, TSC offers technical support on a chargeable basis. Users have the option of calling (800) 859-1763 using their Visa/MasterCard/American Express to receive support at $2.00/min U.S. rate. Registration is recommended, but not required for chargeable service.

Expedited Service

Technical support is given on a first call-first served basis. For convenience, users that demand immediate, expedited response have the option of calling (800) 859-1763 to receive support at a chargeable rate of $2.00/min U.S. rate using their Visa/MasterCard/Am Express. Registration is recommended, but not required for chargeable service.

Out of Date Product Support

To obtain real-time support on products that TouchStone no longer publishes of products replaced by a newer version, users have the option of calling (800) 859-1763 using their Visa/MasterCard/American Express to receive support at $2.00/min U.S. rate. Registration is recommended, but not required for a chargeable service. Registered users may also use one of TouchStone's online services for support at no charge.

Registration

Users may register by mailing in their registration card, faxing the registration card to (714) 969-4444, via the BBS at (714) 969-0688 or by calling (714) 969-7746 and asking for product registration.

{button ,AL(`BBS Support;CompuServe Support;Fax Back Support')} Related Topics

BBS Support

Use your modem to download common problems and solutions on all of our products by calling (714) 969-0688. Downloadable document and utility files are available.

{button ,AL(`Technical Support;CompuServe Support;Fax Back Support')} Related Topics

CompuServe Support

TouchStone CompuServe Information Service/Support:

From any CompuServe prompt, type GO TOUCHSTONE. You may leave an inquiry to receive a response by the following business day. CompuServe subscription information can be obtained by calling (800) 848-8199.

{button ,AL(`BBS Support;Technical Support;Fax Back Support')} Related Topics

Fax Back Support

Common problem and solution documentation may be obtained by calling (714) 536-6195, pressing 1000, listening for the selection of your choice, and entering the correct document number. This is an excellent method when you need help after normal business hours.

{button ,AL(`Technical Support;BBS Support;CompuServe Support')} Related Topics

e.support

TouchStone partnered with the SSPA (Software Support Professionals Association), the foremost organization for service and support professionals, to develop this one-of-a-kind user/vendor support system.

Your Free Technical Support Connection Is Included

Tired of telephone technical support? Then say goodbye to:

- waiting on hold
- limited availability, and
- trying to explain your system's configuration to a support representative.

There's now a faster, easier way to get technical support – and it's called e.support!

With the new e.support program, which comes pre-loaded with PC-cillin II, you'll enjoy universal, electronic access to thousands of hardware and software vendors for all your service needs -- 24 hours a day, seven days a week! Whether you need technical assistance, want to ask a "how to" question, need additional product information, or just want to register new software, e.support makes it easy. The only thing you need is a modem. Once you're plugged in, e.support opens the door to fast, easy technical support.

How Does It Work?

The e.support program uses a simple, fill-in-the-blank format to gather specific details about your problem or request, and then sends the information, along with a system diagnostic file, to the vendor that can help you. This provides support technicians with a detailed description of your problem and shows them exactly how your system is set up, enabling them to provide you with a fast, accurate, and personalized response specifically customized just for you.

Special TouchStone Customer Preview

This version of e.support included in PC-cillin II has been specifically customized to be used for TouchStone products only. You can use it to register any of your TouchStone products, access technical support, or ask a how-to question about any of our products – even e.support itself. A retail public version of e.support, which will connect users to thousands of vendors, will be available in the near future.

Opening the Program

e.support can be launched from PC-cillin II using the e.support command in the Help menu. In this case, you go to the Type of Request screen.

Here, you can choose the type of request that you are going to send – either a Problem Report (typically used to get help for a problem), "How To" Question (where you can ask a vendor how to perform a certain task), Information Request (get details on a given product or vendor), Customer Feedback (state any comments or suggestions to a vendor), and Product Registration (where you can register a product).

For more information of the wide variety of uses for e.support, refer to the program's online Help system, which is accessible through the **Help** button in the lower left of the screen.

Credits

PC-cillin II Development Team
(Listed in alphabetical order)

Documentation and Help
D.C. Native

Graphics Design
Jennifer Shih

Product Managers
Jean Lin
Sal Viveros

Programmers
Aries Chuang
Simon Hung
Mandy Yih

Quality Assurance
Doug Dill
Maggie Lee
Hammud Saway
Edward Tsai
Iris Wu

Senior Programmers
Warren Tsai

User Interface
Joe Lorenzini
Mandy Yih

Special Thanks to
Steve Chang, Eva Chen, Jenny Chen, Daniel Chiang, Terrence Chou, Nicole Hung, Shammi Dingus, Richard Ku, Gina Lee, Cliff Liang, Bob Lowe, and Iris Wu.

compressed files
A single file or series of files that have been compressed into one file using a compression utility such as PKZIP, WINZIP, or LHARC.

icon

A graphical representation of a five-level object--that is, a disk drive, a folder, an application, a document or other object that you can select and open.

drag-and-drop

To position the mouse pointer on top of an item, then depress and hold the main mouse button down while moving the mouse, then release the mouse button.

choose

To use a mouse or keyboard to pick an item that begins an action. You choose commands on menus to perform tasks, and you choose icons to start applications.

click

To press and release a mouse button quickly.

close

To remove a window or dialog box, or quit an application. You can close a window by using the Close command on the Control-menu.

command button

In a window or dialog box, a command carries out an action. A command button often has a label that describes the action it carries out (i.e., Exit or Cancel).

desktop

The screen background for Windows 95 on which windows, icons and dialog boxes appear.

dialog box

A window that appears temporarily to request information. Many dialog boxes have options you must choose before Windows can carry out a command.

folder

Part of a structure for organizing your files on a disk. A folder can contain files and other folders (called sub-folders). The structure of folders and sub-folders on a disk is called a directory tree.

double-click

To rapidly press and release a mouse button twice without moving the mouse. Double-clicking carries out an action, such as starting an application, or moving items from one box to another.

files

A collection of information that has been given a name and is stored on a disk. This information can be a document or an application.

dimmed

Unavailable or disabled. A dimmed button or command is displayed in light gray instead of black, and it cannot be chosen.

list box

Within an application window or dialog box, a type of box that lists available choices--for example, a list of all files in a folder. If all the choices do not fit, there is a scroll bar.

menu bar

The horizontal bar containing the names of the application's menus. It appears below the title bar. For example, File, Options, and Help.

scroll

To move through text or graphics (up, down, left or right) in order to see parts of the file or list than cannot fit on the screen.

virus pattern

A virus pattern is a file that contains a series of virus signature codes (definitions) which is used by PC-cillin II to identify virus infected files.

boot sector

A portion of a disk that contains the coded instructions for the operating system to start the computer.

boot

To start the computer.

boot virus

A virus that infects the boot record program on both hard and floppy disks and/or the master boot record program on hard disks. A boot virus loads into memory before the operating system, taking control of your computer and infecting any floppy disks that you access.

boot record

The first physical sector on a floppy disk or the first logical sector of a hard disk partition. It identifies the disk's architecture (sector size, cluster size, and so forth) and also contains the boot record program.

boot disk

A disk that contains the operating system necessary to start, or boot, the computer.

BBS

An abbreviation for bulletin board service (BBS)--an online service that allows you to send and retrieve messages, electronic mail, and execute file transfers between computer users via a modem.

clean

To remove a virus infection from a floppy disk or the computer's hard disk.

clean boot disk

A diskette that is known not to be infected and contains the coded instructions to start your computer.

detection

Scanning memory and disks for telltale marks or changes indicating that a virus may be present.

device driver

A memory resident program (TSR) that is loaded from CONFIG.SYS or SYSTEM.INI at startup.

TSR

A program that loads itself into random access memory (RAM) and remains there so that it can be instantly activated. The TSR is removed from memory when the computer is turned off.

CONFIG.SYS

A text file containing commands that configure the system's hardware and that load device drivers. The file is automatically executed by the operating system when you start your computer.

download

To transfer a file/files from one computer to another by way of a modem.

executable file

A file containing a program that can be launched. Executable files generally have the following extensions (.BIN, .COM, .DRV, .EXE, .OVL, .OVR, OR .SYS).

infected file

A file that is contaminated with a virus.

known virus

Any virus that PC-cillin II can detect and identify by name.

unknown virus

A virus for which PC-cillin II does not contain a virus definition.

launch

To start or run an application.

load

To start or run an application.

master boot record program

The program that is responsible for directing the computer to load the boot record program from the bootable hard disk.

memory

A storage medium where data or program codes are kept temporarily while being used by the computer. DOS supports up to 640KB of conventional memory. Memory beyond that limit may be accessed as expanded, extended or an upper memory block (UMB).

conventional memory

Up to the first 64- kilobytes (K) of memory on a computer. All MS-DOS- based programs require conventional memory to execute programs.

UMB

Memory just above the MS-DOS 640K limit of conventional memory. Usually in the 640K-1024K range. On an 80386 or 80486 computer, UMBs can be used for running device driver and memory-resident programs.

network

A series of computers and associated hardware (printers and so forth).

operating system

The master control program that is loaded into memory when you start up or boot your computer. It controls and manages all computer operations and programs.

partition table

A table in the master boot record of a hard disk that specifies how the disk is set up, such as the size and location of the partitions, which operating system each partition uses, and which partition the computer will boot from.

pathname

The location of a folder or file on a disk. For example, if a file named (ABC.DOC is stored in the WINWORD folder on drive C:, the pathname for the file is C:\WINWORD\ABC.DOC).

polymorphic

A type of virus that changes its telltale code segments so that it looks different from one infected file to another, therefore making detection more difficult.

stealth virus

A virus that actively seeks to conceal itself from being discovered or is capable of defending itself against attempts to analyze or remove it.

program

An executable file/group of files written for a specific purpose (such as word processing or creating a presentation).

RAM

The computer's working memory that determines the size and number of programs that can be run at the same time, including the amount of data that can be processed instantly.

scan

The systematic search for viruses that is performed by PC-cillin II.

sub-folder

A folder within a folder.

system files

The files that make up the operating system.

taskbar

The desktop component that gives access to the Start menu and currently running programs. PC-cillin II places an icon on the taskbar to remind you that it is enabled.

virus

A self-replicating program written intentionally to alter the way your computer operates without your permission or knowledge.

virus definition

Virus information that allows PC-cillin II to recognize and alert you to the presence of a specific virus.

VxD

A virtual device driver. It is an operating system extension that manages a computer resource. Smart Monitor is an example of VxD.

workstation

A computer that is attached to a network and is not the network server.

write-protect

A disk that cannot be written to. Write-protecting a disks prevents viruses from infecting them. To write-protect a 3.5" disk, slide the lever on the back of the disk to uncover the hole through the disk.

The Check Now button lets you see if there are any new virus pattern files, program updates, virus alerts, virus bulletins, or if an infected file that you sent to the Virus Doctor has been cleaned and is ready to be retrieved.

The Virus Lab button lets you access TouchStone's Internet Virus Lab directly.

In the Active Defense section, you can find out if there is a new virus pattern file, program update, virus alert, virus bulletin, or if an infected file that you sent to our Virus Doctor has been cleaned. If there is, yellow check marks appear next the item (e.g. New Pattern File Available or Virus Alert). Also, instructions that contain hyperlinks to these new items appear in the message box.

Tells whether PC-cillin II's Macro Shield is at work, protecting you from macro viruses.

This drop-down list allows you to specify when a scheduled update to your virus pattern file will occur (e.g., Everyday, Once a Week, Once a Month or Never).

This area allows you to designate the time of day a scheduled update will occur.

If the frequency of a scheduled update is set at once a week, this drop-down list allows you to specify which day of the week the update will occur.

If the frequency of a scheduled update is set at once a month, this drop-down list allows you to specify which day of the month the update will occur.

Determines the method by which PC-cillin II will retrieve the scheduled update, either over the Internet or TouchStone's BBS. For more information, see Scheduling Virus Pattern File Updates.

Click here to subscribe to PC-cillin II's services. This will give you unlimited access to the Virus Lab and virus pattern file updates.

To unlock a subscription, click on this button. For more information, see Unlocking a Subscription.

NCSA Certification

The National Computer Security Association (NCSA) certification scheme is designed to focus on the real threat to corporate PCs: those viruses known to be in the wild. In order to be certified, a product must pass the following tests:

1. Certified products must detect 100% of all those viruses defined as 'in the wild' according to the upper part of the Wild List. As new viruses are discovered all the time, the Wild List used is the one which was current two months prior to the date of the certification test.

2. Certified products must still detect a minimum of 90% of the NCSA virus 'Zoo', made up of samples of some of the 6000+ other viruses known.

These tests are carried out with the product running its default mode of operation, with the exception of using any appropriate logging facilities.

Certification Maintenance

Once a product is certified, NCSA will attempt to recertify the product a minimum of 4 times per year. Each certification attempt will be carried out without the prior knowledge of the developer.

This helps to ensure that every release of the product is capable of meeting the certification criteria, not just a special 'certification' version.

If a product fails either test I or II, the vendor will be given 7 days to supply a fix for the problem, and make this fix publicly available. If this time limit is not met, the product will be removed from the certified product list available from this Web site. This list will be maintained in such away that a product's certification history (passes and failures) will be visible.

Once a product has been decertified, certification can only be regained when the vendor ships through its normal distribution channel a version of the product which is certifiable. A special fix just sent to NCSA for testing is not acceptable.

Collection Management

One of the most important factors to consider when carrying out a set of detection tests on anti-virus software is the way in which the virus library is managed. It is also vital to know which vendors (if any) have access to the actual test samples used, and the way in which the library is created.

No sample used in the NCSA 'in the wild' test-set is sent out to any vendor. However, should a virus be missed during a certification attempt, a replicant of that sample (note that this is not a copy of the actual sample) will be sent out to the vendor for inclusion in the next release of the product. This process ensures that vendors have reliable detection algorithms for each virus in the collection.

In the case of a polymorphic virus, multiple copies of each virus is used, to ensure that the product tested can detect that virus with accuracy. Copies of individual replications of each virus from within this test-set are not made available to vendors; thus, the test is carried out against an 'unseen' collection of files. In order to pass this test, the product must detect every replication in the test-set.

All viruses in the collection are attached to standard Goat files, ensuring that no 'first generation' samples are in the collection. Furthermore, should a virus be missed during certification, a check is made to make certain that the file is not corrupted and is capable of replication.

NCSA Certification Web Page and Address

The NCSA Web page listed below will always contain the latest in certification information and testing scheme.

http://www.ncsa.com/avpdcert.html

National Computer Security Association
10 S. Courthouse Avenue
Carlisle, PA 17013
USA
http://www.ncsa.com
(717) 258-1816

Frequently Asked Questions (FAQs)

The following topics provide answers to questions that are frequently cross out technical support desk. Each topic addresses a grab bag of issues that may help you solve a problem without having to call technical support.

Questions About Program Execution

A list of questions is provided below.

Post Installation Problems

Q: After I installed PC-cillin 95, I cannot access the PC-cillin 95 program or view the Read Me file, an error comes up stating "Can't find file C:\WINDOWS\SYSTEM\MFC30.DLL." What is wrong?

A: MFC30.DLL is a file installed by Windows 95. If it is missing from your computer, any program that makes a call to the Microsoft Function Class library may not work correctly. PC-cillin 95 does make calls to this library, as does the Microsoft WordPad, which the Read Me icon starts. We suggest you contact Microsoft Technical Support at (206) 635-7000 for assistance in replacing this file.

One-Button Updates

Q: I'm trying to download the Virus Pattern File from the one click Internet button. I receive a message, "Failed to connect to host!"

A: In order to make an Internet connection, you must have an Internet Service Provider set up in Window 95. This is done through the TCP/IP setup, we suggest you contact your Internet service provider (or Microsoft) for help.

Q: When I try to update my virus pattern file with the BBS UPDATE button, I get the message "Failed To Connect!" What is the problem?

A: That message indicates that either the BBS is not answering the phone or the BBS is busy.

Q: When I try to update the virus pattern file with the Internet Update button, I get an error, "Windows Socket error, Couldn't create socket." Why isn't the button working?

A: This is a problem with either a corrupt or missing WSOCK32.DLL file. We suggest you contact Microsoft's Windows 95 Technical Support at (206) 635-7000 for help in replacing the WSOCK32.DLL file. For those with access to Microsoft's Knowledge Base on CompuServe, download document Q145703, dated 2/7/96 for further information on WSOCK32.DLL problems. The EXTRACT document (Q129605, dated 1/23/96) will be of help to those who need instructions on EXTRACT.EXE.

Working with Dr. Solomon's Anti-Virus Program

Q: If I'm running Dr. Solomon's Anti-Virus program, will it conflict with PC-cillin?

A: Yes. When Dr. Solomon's Winguard VXD is loaded, PC-cillin will not detect any file type viruses.

WSOCK32.DLL

Q: When PC-cillin 95 starts, I get an error box stating "WSOCK32.DLL FILE CANNOT START, CHECK THE FILE TO DETERMINE THE PROBLEM". What is the problem?

A: The WSOCK32.DLL is either corrupt or missing. We suggest you contact Microsoft Windows 95 Technical Support at (206) 635-7000 for help in replacing the WSOCK32.DLL file. For those with access to Microsoft's Knowledge Base on CompuServe, download document Q145703, dated 2/7/96 for further information on WSOCK32.DLL problems. The EXTRACT document (Q129605, dated 1/23/96) will be of help to those who need instructions on EXTRACT.EXE.

Modem Connection in Smart Monitor

Q: My modem connection does not display activity in the Smart Monitor Window.

A: The Smart Monitor will only monitor certain Windows communications programs. A future update will add additional programs that are not currently monitored.

Questions About Viruses

There are a lot of questions that pertain to viruses and their effects on your computer. For this reason, the questions have been separated into categories, which you can choose:

Where can viruses hide?

Listed below are questions that pertain to where viruses can hide:

CMOS Memory

Q: Can a virus hide in a PC's CMOS memory?

A: No. The CMOS RAM in which system information is stored and backed up by batteries is ported, not addressable. That is, in order to get anything out, you use I/O instructions. Anything stored there is not directly sitting in memory. Nothing in a normal machine loads the data from there and executes it, so a virus that "hid" in the CMOS RAM would still have to infect an executable object of some kind in order to load and execute whatever it had written to CMOS. A malicious virus can of course alter values in the CMOS as part of its payload, but it cannot spread through or hide in the CMOS.

Extended or Expanded RAM

Q: Can a virus hide in Extended or Expanded RAM?

A: Theoretically yes, although no such viruses are known yet. However, even if they are created, they must partly resident in conventional RAM; they cannot reside entirely in Extended or Expanded RAM.

Upper or High Memory

Q: Can a virus hide in Upper or High Memory?

A: Yes, it is possible to construct a virus that reside in Upper Memory (640K to 1024K) or High Memory (1024K to 1088K). A few currently known viruses (e.g., EDV) do hide in Upper Memory.

It might be thought that there is no point in scanning in these areas for any viruses other than those that are specifically known to inhabit them. However, there are cases when even ordinary viruses can be found in Upper Memory. Suppose that a conventional memory-resident virus infects a TSR program and this program is loaded high by the user (for instance, from AUTOEXEC.BAT). Then the virus code will also reside in Upper Memory. Therefore, an effective scanner must be able to scan this part of memory for viruses, too.

What can a virus infect?

Listed below are questions that pertain to what components of your computer can be infected by a virus:

Infecting Windows 95

Q: Can DOS and Windows 3.1 viruses infect a Windows 95 system?

A: Yes. Currently about 70-80% of the existing DOS and Windows 3.1 virus can infect Windows 95 system.

Infecting Non-Bootable Disks

Q: Can boot sector viruses infect non-bootable floppy disks?

A: Any diskette that has been properly formatted contains an executable program in the boot sector. If the diskette is not "bootable," all that the boot sector does is print a message like *"Non-system disk or disk error; replace and strike any key when ready,"* but it's still executable and still vulnerable to infection. If you accidentally turn on your machine with a "non-bootable" diskette in the drive, and see that message, it means that any boot virus that may have been on that diskette has run and had the chance to infect your computer. So when thinking about viruses, the word "bootable" or "non-bootable" is really misleading. All formatted diskettes are capable of carrying a virus.

Infecting Data Files

Q: Can a virus infect data files?

A: Some viruses (e.g., Frodo, Cinderella, DataCrime) modify non-executable files. However, in order to spread, the virus must be executed. Therefore, the "infected" non-executable files cannot be sources of further infection.

Note that it is not always possible to make a sharp distinction between executable and non-executable files. One person's code is another person's data and vice versa. Some files that are not directly executable contain code or data that can, under some conditions, be executed or interpreted.

Some examples from the PC world are OBJ files, libraries, device drivers, source files for any compiler or interpreter, macro files for some packages like MS Word and Lotus 1-2-3, and many others. Currently, there are viruses that infect boot sectors, master boot records, COM files, EXE files, BAT files, and device drivers, although any of the objects mentioned above can theoretically be used as an infection carrier. PostScript files can also be used to carry a virus, although no known viruses that currently do so.

Infecting Cross Platforms

Q: Can viruses spread from one type of computer to another (e.g., from a PC to a Mac)?

A: The simple answer is that no currently known virus can do this. Although the disk formats may be the same (e.g., Atari ST and DOS), the machines interpret the code differently. For example, the Stoned virus cannot infect an Atari ST as the ST cannot execute the virus code in the boot sector. The Stoned virus contains instructions for the 80x86 family of CPUs, which the 680x0-family CPU (Atari ST) can't understand or execute.

The more general answer is that such viruses are possible, but unlikely. Such a virus would be quite a bit larger than current viruses and might well be easier to find. Additionally, the low incidence of cross-machine sharing of software means that any such virus would be unlikely to spread -- it would be a poor environment for virus growth.

Running on Non-DOS Machines

Q: Can DOS viruses run on non-DOS machines (e.g., Mac, Amiga)?

A: In general, no. However, on machines running DOS emulators (either hardware or software based), DOS viruses, just like any DOS program, may function. These viruses would be subject to the file access controls of the host operating system. An example is when running a DOS emulator such as VP/ix under a 386 UNIX environment, DOS programs are not permitted access to files that the host UNIX system does not allow them to. Thus, it is important to administer these systems carefully.

Infecting Mainframe Computers

Q: Can mainframe computers be susceptible to computer viruses?

A: Yes. Numerous experiments have shown that computer viruses spread very quickly and effectively on mainframe systems. However, to our knowledge, no non-research computer virus has been seen on mainframe systems. (The Internet worm of November 1988 was not a computer virus by most definitions, although it had some virus-like characteristics.) Computer viruses are actually a special case of something else called "malicious logic," and other forms of malicious logic -- notably Trojan horses -- are far quicker, more effective, and harder to detect than computer viruses. Nevertheless, on personal computers, many more viruses are written than Trojans. There are two reasons for this: (1) Since a virus propagates, the number of users to which damage can be caused is much greater than in the case of a Trojan; (2) It's almost impossible to

trace the source of a virus since it's not attached to any particular program.

DOS Viruses Working Under Windows

Q: Can normal DOS viruses work under MS Windows?

A: Most of them cannot. A system that runs exclusively MS Windows is, in general, more virus-resident. Viruses are not compatible with the memory management in Windows. Furthermore, most of the existing viruses will damage the Windows applications if they try to infect them as normal EXE files. The damaged applications will stop working and this will alert the user that something is wrong.

Don't mistake being virus-resistant for being virus-proof, though. For instance, most of the well-behaved resident viruses that infect only .COM files (Cascade is an excellent example) will work perfectly in a DOS window. All non-resident COM infectors will be able to run and infect, too. And currently there exists at least one Windows-specific virus that is able to properly infect Windows applications (it is compatible with the new EXE file format). This virus is named WNVIR14.

Any low level trapping of Interrupt 13, as by resident boot sector and MBR viruses, can also affect Windows operations, particularly if protected disk access (32BitDiskAccess=ON in SYSTEM.INI) is used.

How many viruses are there?

It's impossible to give an exact number because five to seven new viruses are literally created every day. Furthermore, different anti-virus researchers use different criteria to decide whether two viruses are different or the same. Some count viruses as different if they differ by at least one bit in their non-variable code. Others group the viruses in families and do not count the closely related variants in one family as different viruses.

Making a rough estimate, as of September 1995, there were about approximately 6000+ IBM PC viruses, about 150 Amiga viruses, about 65+ Macintosh viruses, about a dozen Acorn Archimedes viruses, several Atari ST viruses, and a few Apple II viruses.

However, very few of the existing viruses are widespread. For instance, only about three dozen of the known IBM PC viruses are causing most of the reported infections. The virus that most people are concerned about the "in the wild virus" or "common virus."

Why do viruses spread so quickly?

This is a very complex issue. Most viruses don't spread very quickly. Those that do spread widely are able to do so for a variety of reasons. A large target population (i.e., millions of compatible computers) helps. A large virus population helps. Vendors whose quality assurance mechanisms rely on, for example, outdated scanners help. Users who insert new software into their systems without making any attempt to test for viruses help. All of these things are factors.

The Word macro virus that was just recently discovered can spread very fast due to the fact that many people are not aware of these kinds of virus and people sharing .doc file through out an organization or through email are more common.

When seeking assistance for a virus infection, what information should I have ready?

People frequently post messages to our CompuServe Forum and BBS requesting assistance on a suspected virus problem. To better answer the user's questions we recommend that users provide us with the following information when requesting assistance:

- The name of the virus (if known);
- The name of the program that detected it;
- The version of the program that detected it;
- Any other anti-virus software that you are running and whether it has been able to detect the virus or not. And if yes, by what name did it call it;
- Your software and hardware configuration (computer type, kinds of diskette drives), amount of memory and configuration (extended/expanded/conventional), TSR programs and device drivers used, OS version, etc.)

It is helpful if you can use more than one scanning program to identify a virus -- and to say which scanner gave which identification. However, some scanning programs leave "signatures" in memory that will confuse others. So, it is best to do a "cold reboot" between runs of successive scanners, particularly if you are getting confusing results.

How often should we upgrade our anti-virus tools to minimize software and labor costs, maximizing our protection? And what is a good anti-virus software program?

Anti-viral software is a kind of insurance, and these type of calculations are difficult. However, before deciding to purchase an anti-virus program, you should consider the following: the general ‘‘style’’ of the software and the signatures that scanners use to identify viruses. Scanners should be updated more frequently than other software, and it is probably a good idea to update your set of signatures at least once every two months.

TouchStone offers one-button virus pattern file updates via our web site, BBS, by calling technical support, or through our CompuServe Forum.

Of course, not every anti-virus product is effective against all viruses, even if upgraded regularly. Thus, do not depend on the fact that you have upgraded your product recently as a guarantee that your system is free of viruses! One needs to always practice safe computing!

I think the virus Stoned has infected my system. What should I do?

Listed below are questions that pertain to the Stoned virus:

Q: I was told that the Stoned virus displays the text *''Your PC is now Stoned''* at boot time. I have been infected by this virus several times, but have never seen the message. Why?

A: The ''original'' Stoned message was *''Your PC is not Stoned!''*, where the ''.'' represents the ''bell'' character (ASCII 7 or ''PC speaker beep'').
The message is displayed with a probability of 1 in 8 only when a PC is booted from an infected diskette. When booting from an infected hard disk, Stoned never displays this message.
Recently, versions of Stoned with no message whatsoever or only the leading bell character have become very common. These versions of Stoned are likely to go unnoticed by all but the most observant, even when regularly booting from infected diskettes.
Contrary to some reports, the Stoned virus does not display the message ''*LEGALIZE MARIJUANA,''* although such a string is quite clearly visible in the boot sectors of diskettes infected with the ''original'' version of Stoned in standard'' PCs.

Q: I was infected by both Stoned and Michelangelo. Why has my computer become unbootable? And why, each time I run my favorite scanner, does it find one of the viruses and say that it is removed, but when I run it again, it says that the virus is still there?

A: These two viruses store the original Master Boot Record at one and the same place on the hard disk. They do not recognize each other. Therefore, a computer can become infected with both of them at the same time.
The first of these viruses that infects the computer will overwrite the Master Boot Record with its body and store the original MBR at a certain place on the disk. So far, this is normal for a boot-record virus. But if the other virus also infects the computer, it will replace the MBR (which now contains the virus that has come first) with its own body, and stores what it believes is the original MBR (but in fact, its the body of the first virus) AT THE SAME PLACE on the hard disk, thus OVERWRITING the original MBR. When this happens, the contents of the original MBR are lost. Therefore, the disk becomes non-bootable.
When a virus removal program inspects such a hard disk, it will see the SECOND virus in the MBR and will try to remove it by overwriting it with the contents of the sector where this virus normally stores the original MBR. However, now this sector contains the body of the FIRST virus. Therefore, the virus removal program will install the first virus in trying to remove the second. In all probability, it will not wipe out the sector where the (infected) MBR has been stored.

How do DOS viruses interact with OS/2?

Listed below are questions that pertain to how DOS viruses interact with OS/2:

Q: Can a DOS virus survive and spread on an OS/2 system using the HPFS file system?

A: Yes, both file-infecting and boot sector viruses can infect HPFS partitions. File-infecting viruses function normally and can activate and do their dirty deeds, and boot sector viruses can prevent OS/2 from booting if the primary bootable partition is infected. Viruses that try to directly address disk sectors cannot function because OS/2 prevents this activity.

Q: Under OS/2 2.0, could a virus infected DOS session infect another DOS session?

A: Each DOS program is run in a separate Virtual DOS Machine (their memory spaces are kept separated by OS/2). However, any DOS program has almost complete access to the files and disks, so infection can occur if the virus infects files; any other DOS session that executes a program infected by a virus that makes itself memory resident would itself become infected. Bear in mind that all DOS sessions share the same copy of the command interpreter. Therefore, if it becomes infected, the virus will be active in all DOS sessions.

When am I at risk?

Listed below are questions that pertain to certain things you can do or should not do as it relates to viruses:

Disinfecting Files

Q: Some people say that disinfecting files is a bad idea. Is that true?

A: Disinfecting a file is completely "safe" only if the disinfecting process restores the non-infected state of the object completely. That is, not only the virus must be removed from the file, but the original length of the file must be restored exactly as well as its time and date of last modification, all fields in the header, etc. Sometimes it is necessary to be sure that the file is placed on the same clusters of the disk that it occupied prior to infection. If this is not done, then a program that uses some kind of self-checking or copy protection may not function properly, if at all.

None of the currently available disinfecting programs completely restore a file to its original state. For instance, because of the bugs that exist in many viruses, some of the information of the original file is destroyed and cannot be recovered. Other times, it is even impossible to detect that this information has been destroyed and to warn the user. Furthermore, some viruses corrupt information very slightly and in a random way (e.g., Nomenklatura and Phoenix), so that it is not even possible to tell which files have been corrupted.

Therefore, it is usually better to replace the infected objects with clean backups, provided you are certain that your backups are not infected. You should try to disinfect files only if they contain some valuable data that cannot be restored from backups or compiled from their original source.

Avoiding Shareware/Free Software/Games

Q: Can I avoid viruses by avoiding shareware/free software/games?

A: No. There are many documented instances in which even commercial "shrink wrap" software was inadvertently distributed containing viruses. Avoiding shareware, freeware, games, etc. only isolates you from a vast collection of software (some of it very good, some of it very bad, most of it in between...). The important thing is not to avoid a certain type of software, but to be cautious of ANY AND ALL newly acquired software. Simply scanning all new software media for known viruses would be rather effective at preventing virus infections, especially when combined with some other prevention/detection strategy such as integrity management of programs.

The DIR Command

Q: Can I contract a virus on my PC by performing a "DIR" of an infected floppy disk?

A: If you assume that the PC you are using is virus free before you perform the DIR command, then the answer is no. However, when you perform a DIR, the contents of the boot sector of the diskette are loaded into a buffer for use when determining disk layout among other things, and certain anti-virus products will scan these buffers. If a boot sector virus has infected your diskette, the virus code will be contained in the buffer, which may cause some anti-virus packages to give the message *"XYZ virus found in memory, shut down computer immediately."* In fact, the virus is not a threat at this point since control of the CPU is never passed to the virus code residing in the buffer. But, even though the virus is not really a threat, this message should not be ignored. If you get a message like this, then reboot from a clean DOS diskette, scan your hard-drive, and find no virus, you know that the false positive was caused by the fact that the infected boot-sector was loaded into a buffer. In this case, the diskette should be appropriately disinfected before use. The use of DIR will not infect a clean system, even if the diskette it is being performed on does contain a virus.

Copying Infected Files to Clean PC

Q: Is there any risk in copying data files from an infected floppy disk to a clean PC's hard disk?

A: Assuming that you did not boot or run any executable programs from the infected disk, the answer is generally no. There are two caveats: 1) you should be somewhat concerned about checking the integrity of these data files as they may have been destroyed or altered by the virus; 2) if any of the "data" files are interpretable as executable by some other program (such as a Lotus macro), then these files should be treated as potentially malicious until the symptoms of the infection are known. The copying process itself is safe (given the above scenario). However, you should be concerned with what type of files are being copied to avoid introducing other problems.

I was infected by the Jerusalem virus and disinfected the infected files with my favorite anti-virus program. However, WordPerfect and some other programs still refuse to work. Why?

The Jerusalem virus and WordPerfect 4.2 program combination is an example of a virus and program that cannot be completely disinfected by an anti-virus tool. In some cases such as this one, the virus will destroy code by overwriting it instead of appending itself to the file. The only solution is to re-install the programs from clean (non-infected) backups or distribution media.